RayTalk

802.11n/g/b

High Speed Wireless Router

RA-M100

11n/g/b (1Tx1R)
Wireless Router

RA-M100Plus

11n/g/b (1Tx1R) 3G
Wireless Router

RA-M200

11n/g/b (2Tx2R)
Wireless Router

User's Manual

Version 1.0

Copyright © RayTalk Industries. Tutti i diritti riservati.

Declaration of Conformity

We, the under signed

RayTalk Industries Srl
Via Nicolino di Galasso 19
47899 Serravalle
Republic of SAN MARINO
Tel: +378 0549 901170
Fax: +378 0549 900890
Contact: Mr. Gianluigi Savioli
E-Mail: gianluigi.savioli@raytalk.com

declare under our own responsibility that the product :

Brand Name	RayTalk
Model	RA-M100
Descriptions	IEEE 802.11b/g/n Wireless Access Point / Router
Applicant	RayTalk Industries Srl

to which this declaration refers conforms with the relevant standards:

Standard	**Issue date**
EN 60950-1	2006
EN 300 328 V1.7.1.	2006-10
EN 55022 CLASS B	2006
EN 55024	1998+A1:2001+A2:2003
EN 301 489-1 V1.6.1	2005-09
EN 301 489-17 V1.2.1	2002-08

We hereby declare that the essential radio tests suites have been carried out and that the above named product is in conformity with all the essential requirements of R&TTE Directive 1999/5/EC.

The technical construction file as required by the Conformity Assessment procedure is kept at the address of the applicant.

CE 1177 !

The product RayTalk RA-M100 has been tested and found to comply with the stated standards which are required by the article 6.4 of the R&TTE Directive of 99/5/EEC.

This equipment may be operated in: IT

Note: the use of the present equipment in the Italian regulation is ruled by the following directives:

- ***D.Lgs 1.8.2003, n.259 articles 104 and 105 for private use***
- ***D.M. 28.5.2003 and further modifications for R-LAN and telecommunication services with public access***

Gianluigi Savioli / Amministratore Unico
RayTalk Industries Srl
Date: 9TH JULY 2010

 Copyright © RayTalk Industries. Tutti i diritti riservati.

Declaration of Conformity

We, the under signed

RayTalk Industries Srl
Via Nicolino di Galasso 19
47899 Serravalle
Republic of SAN MARINO
Tel: +378 0549 901170
Fax: +378 0549 900890
Contact: Mr. Gianluigi Savioli
E-Mail: gianluigi.savioli@raytalk.com

declare under our own responsibility that the product :

Brand Name	RayTalk
Model	RA-M100Plus
Descriptions	IEEE 802.11b/g/n Wireless Access Point / Router
Applicant	RayTalk Industries Srl

to which this declaration refers conforms with the relevant standards:

Standard	**Issue date**
EN 60950-1	2006
EN 300 328 V1.7.1.	2006-10
EN 55022 CLASS B	2006
EN 55024	1998+A1:2001+A2:2003
EN 301 489-1 V1.6.1	2005-09
EN 301 489-17 V1.2.1	2002-08

We hereby declare that the essential radio tests suites have been carried out and that the above named product is in conformity with all the essential requirements of R&TTE Directive 1999/5/EC.

The technical construction file as required by the Conformity Assessment procedure is kept at the address of the applicant.

CE 1177 !

The product RayTalk RA-M100Plus has been tested and found to comply with the stated standards which are required by the article 6.4 of the R&TTE Directive of 99/5/EEC.

This equipment may be operated in: IT

Note: the use of the present equipment in the Italian regulation is ruled by the following directives:

- ***D.Lgs 1.8.2003, n.259 articles 104 and 105 for private use***
- ***D.M. 28.5.2003 and further modifications for R-LAN and telecommunication services with public access***

Gianluigi Savioli / Amministratore Unico
RayTalk Industries Srl
Date: 9TH JULY 2010

Copyright © RayTalk Industries. Tutti i diritti riservati.

Declaration of Conformity

We, the under signed

RayTalk Industries Srl
Via Nicolino di Galasso 19
47899 Serravalle
Republic of SAN MARINO
Tel: +378 0549 901170
Fax: +378 0549 900890
Contact: Mr. Gianluigi Savioli
E-Mail: gianluigi.savioli@raytalk.com

declare under our own responsibility that the product :

Brand Name	RayTalk
Model	RA-M200
Descriptions	IEEE 802.11b/g/n Wireless Access Point / Router
Applicant	RayTalk Industries Srl

to which this declaration refers conforms with the relevant standards:

Standard	**Issue date**
EN 301 489-1 V1.8.1	2008-04
EN 301 489-17 V2.1.1	2009-05
EN 60950-1	2006 + A11:2009
EN 300 328 V1.7.1.	2006-10

We hereby declare that the essential radio tests suites have been carried out and that the above named product is in conformity with all the essential requirements of R&TTE Directive 1999/5/EC.

The technical construction file as required by the Conformity Assessment procedure is kept at the address of the applicant.

CE 1177!

The product RayTalk RA-M200 has been tested and found to comply with the stated standards which are required by the article 6.4 of the R&TTE Directive of 99/5/EEC.

This equipment may be operated in: IT

Note: the use of the present equipment in the Italian regulation is ruled by the following directives:

- ***D.Lgs 1.8.2003, n.259 articles 104 and 105 for private use***
- ***D.M. 28.5.2003 and further modifications for R-LAN and telecommunication services with public access***

Gianluigi Savioli / Amministratore Unico
RayTalk Industries Srl
Date: 29TH JULY 2010

 Copyright © RayTalk Industries. Tutti i diritti riservati.

Table of Contents

TERMINOLOGY V

1 INTRODUCTION 1

1.1 PACKAGE CONTENTS 1
1.2 PRODUCT FEATURES 1
1.3 RA-M100 PANEL DESCRIPTION 3
1.4 RA-M100 INTERFACE DESCRIPTION 4
1.1 RA-M100PLUS PANEL DESCRIPTION 5
1.2 RA-M100PLUS INTERFACE DESCRIPTION 6
1.3 RA-M200 PANEL DESCRIPTION 7
1.4 RA-M200 INTERFACE DESCRIPTION 8

2 INSTALLATION 9

2.1 HARDWARE INSTALLATION 9
2.2 SOFTWARE INSTALLATION 9

3 SOFTWARE CONFIGURATION 10

3.1 PREPARE YOUR PC TO CONFIGURE THE WLAN BROADBAND ROUTER 10
3.2 CONNECT TO THE WLAN BROADBAND ROUTER 12
3.3 MANAGEMENT AND CONFIGURATION ON THE WLAN BROADBAND ROUTER 12
3.3.1 Status 12
3.3.2 Setup Wizard 15
I Operation Mode 15
II Time Zone Setting 16
III LAN Interface Setup 16
IV WAN Interface Setup 17
V Wireless Basic Settings 17
VI Wireless Security Setup 18
3.3.3 Operation Mode 19
3.3.4 Wireless - Basic Settings 20
3.3.5 Wireless - Advanced Settings 22
3.3.6 Wireless - Security Setup 24
3.3.7 Wireless - Access Control 26
3.3.8 WDS Settings 27
I WDS Security Setup 28

 Copyright © RayTalk Industries. Tutti i diritti riservati.

Requirement: Set [Wireless]->[Basic Settings]->[Mode]->AP+WDS 28
II WDS AP Table 29
3.3.9 Wireless Mesh Network Settings (only RA-M100Plus) 30
3.3.10 Site Survey 31
3.3.11 WPS 32
3.3.12 Schedule 33
3.3.13 LAN Interface Setup 34
I Static DHCP Setup 35
3.3.14 WAN Interface Setup 37
I Static IP 37
II DHCP Client 39
III PPPoE 41
IV PPTP 44
V L2TP 47
VI GSM 3.5G (RA-M100Plus only) 50
3.3.15 Firewall - Port Filtering 52
3.3.16 Firewall - IP Filtering 53
3.3.17 Firewall - MAC Filtering 55
3.3.18 Firewall - Port Forwarding 56
3.3.19 Firewall – URL Filtering 57
3.3.20 Firewall - DMZ 58
3.3.21 Routing Setup 59
3.3.22 QoS 60
3.3.23 USB Storage 62
3.3.24 Management - Statistics 64
3.3.25 Management - DDNS 65
3.3.26 Management - Time Zone Setting 66
3.3.27 Management – Denial-of-Service 67
3.3.28 Management - Log 68
3.3.29 Management - Upgrade Firmware 69
3.3.30 Management - Save/ Reload Settings 70
3.3.31 Management – Watchdog 71
3.3.32 Management - Reboot 71
3.3.33 Management – Password Setup 72
3.3.34 Logout 73

 Copyright © RayTalk Industries. Tutti i diritti riservati.

FREQUENTLY ASKED QUESTIONS (FAQ) 74

3.1 What and how to find my PC's IP and MAC address? 74
3.2 What is Wireless LAN? 74
3.3 What are ISM bands? 74
3.4 How does wireless networking work? 74
3.5 What is BSSID? 75
3.6 What is ESSID? 76
3.7 What are potential factors that may causes interference? 76
3.8 What are the Open System and Shared Key authentications? 76
3.9 What is WEP? 76
3.10 What is Fragment Threshold? 77
3.11 What is RTS (Request To Send) Threshold? 77
3.12 What is Beacon Interval? 78
3.13 What is Preamble Type? 78
3.14 What is SSID Broadcast? 78
3.15 What is Wi-Fi Protected Access (WPA)? 78
3.16 What is WPA2? 79
3.17 What is 802.1x Authentication? 79
3.18 What is Temporal Key Integrity Protocol (TKIP)? 79
3.19 What is Advanced Encryption Standard (AES)? 79
3.20 What is Inter-Access Point Protocol (IAPP)? 80
3.21 What is Wireless Distribution System (WDS)? 80
3.22 What is Universal Plug and Play (uPNP)? 80
3.23 What is Maximum Transmission Unit (MTU) Size? 80
3.24 What is Clone MAC Address? 80
3.25 What is DDNS? 81
3.26 What is NTP Client? 81
3.27 What is VPN? 81
3.28 What is IPSEC? 81
3.29 What is WLAN Block Relay Between Clients? 81
3.30 What is WMM? 81
3.31 What is WLAN ACK TIMOUT? 81
3.32 What is Modulation Coding Scheme (MCS)? 82
3.33 What is Frame Aggregation? 82
3.34 What is Guard Intervals (GI)? 82
3.35 What is Mesh protocol? 82
3.36 Which 3.5G Devices are compatible with RA-M100Plus? 83

 Copyright © RayTalk Industries. Tutti i diritti riservati.

4 CONFIGURATION EXAMPLES 84

4.1 EXAMPLE ONE – PPPOE ON THE WAN 84

4.2 EXAMPLE TWO – FIXED IP ON THE WAN 87

4.3 EXAMPLE THREE (RA-M100PLUS ONLY) – 3.5G ON THE WAN 90

RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

Terminology

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AP	Access Point
CCK	Complementary Code Keying
CSMA/CA	Carrier Sense Multiple Access/ Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access/ Collision Detection
DDNS	Dynamic Domain Name Server
DH	Diffie-Hellman Algorithm
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
FCC	Federal Communications Commission
FTP	File Transfer Protocol
GI	Guard Intervals
IAPP	Inter Access Point Protocol
IEEE	Institute of Electrical and Electronic Engineers
IKE	Internet Key Exchange
IP	Internet Protocol
ISM	Industrial, Scientific and Medical
LAN	Local Area Network
MAC	Media Access Control
MCS	Modulation Coding Scheme
MD5	Message Digest 5
NAT	Network Address Translation
NT	Network Termination
NTP	Network Time Protocol
PPTP	Point to Point Tunneling Protocol
PSD	Power Spectral Density
RF	Radio Frequency
SHA1	Secure Hash Algorithm
SNR	Signal to Noise Ratio

 Copyright © RayTalk Industries. Tutti i diritti riservati.

SSID	Service Set Identification
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
UPNP	Universal Plug and Play
VPN	Virtual Private Network
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy
WISP	Wireless Internet Service Provider
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup

 Copyright © RayTalk Industries. Tutti i diritti riservati.

1 Introduction

The Wireless LAN Broadband Routers **RayTalk RA-M100**, **RA-M100Plus** and **RA-M200** are affordable IEEE 802.11b/g/n wireless LAN broadband router solutions for setting SOHO and enterprise standard high performance, secure, manageable and reliable WLAN. This document describes the steps required for the initial IP address assign and other WLAN router configuration. The description includes the implementation of the above steps.

1.1 Package contents

The package of the WLAN Broadband Router includes the following items,

- ✓ WLAN Broadband Router **RA-M100**, **RA-M100Plus** or **RA-M200**
- ✓ AC to DC power adapter
- ✓ Documentation and CD
- ✓ RJ-45 Cable Line

1.2 Product Features

- ➢ Complies with IEEE 802.11b/g/n standard for 2.4GHz Wireless LAN.
- ➢ Compatible with IEEE 802.11n Specifications provides wireless speed up to 150Mbps data rate (RA-M100 and RAM100Plus) or 300Mbps (RA-M200).
- ➢ Compatible with IEEE 802.11g high rate standard to provide wireless Ethernet speeds of 54Mbps data rate.
- ➢ Maximizes the performance and ideal for media-centric applications like streaming video, gaming and Voice over IP technology.
- ➢ Supports multi-operation (bridge/gateway/WISP) modes between wireless and wired Ethernet interfaces.
- ➢ Supports WPS, 64-bit and 128-bit WEP, WPA, WPA2 encryption/decryption and WPA with Radius function to protect the wireless data transmission.
- ➢ Supports IEEE 802.1x Authentication.
- ➢ Support Wi-Fi Protected Access Authentication with Radius and Pre-Shared Key mode.
- ➢ Supports Inter-Access Point Protocol (IAPP).
- ➢ Supports Wireless Distribution System (WDS).
- ➢ Supports IEEE 802.3x full duplex flow control on 10/100M Ethernet interface.
- ➢ Supports DHCP server to provide clients auto IP addresses assignment.
- ➢ Supports DHCP client for WAN interface auto IP address assignment from ISP.
- ➢ Supports PPPoE on WAN interface.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

- Supports PPTP Client on Ethernet WAN interface.
- Supports L2TP Client on Ethernet WAN interface.
- Supports clone MAC address function.
- Supports firewall security with Port filtering, IP filtering, MAC filtering, Port forwarding, DMZ hosting and URL filtering functions.
- Supports WEB based management and configuration.
- Supports UPnP for automatic Internet access.
- Supports Dynamic DNS service.
- Supports NTP client service.
- Supports Log table and remote Log service.
- Support Setup Wizard mode.
- Support DoS (Denial of Service) function.
- Support WMM (Wireless Multimedia Multimedia) function.

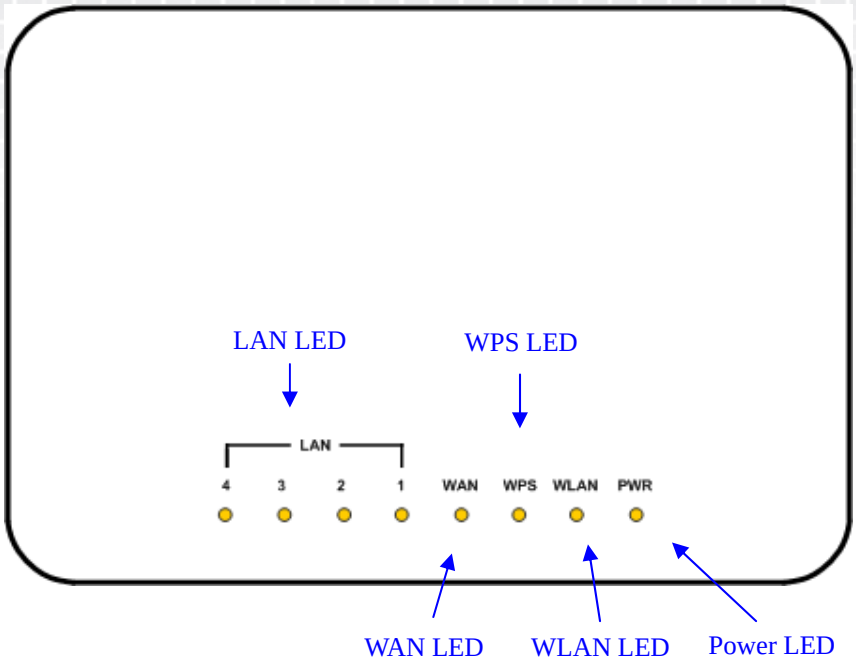
Further RA-M100Plus Special Features

- USB port for 3G Dongle or external storage.
- 2G/3G WAN Connection.
- USB Storage (external Hard Disk or Flash Drive) for Network File Sharing function.
- USB Storage (external Hard Disk or Flash Drive) for FTP Server function.
- Support for USB storage tool.
- Mesh topology.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

1.3 RA-M100 Panel Description

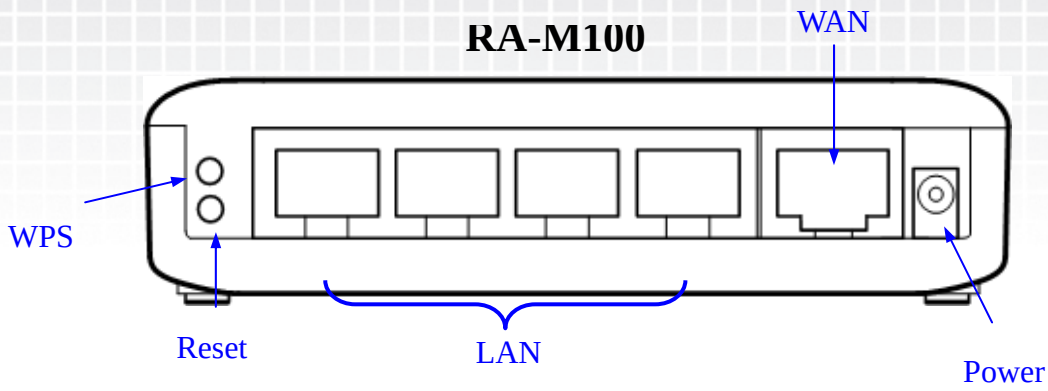
RA-M100



LED Indicator	State	Description
Power LED	On	The WLAN Broadband Router is powered on.
	Off	The WLAN Broadband Router is powered off.
WLAN LED	Flashing	Data is transmitting or receiving on the antenna.
	Off	No data is transmitting or receiving on the antenna.
WPS LED	Flashing	The WPS feature is Enabled.
	Off	The WPS feature is Disabled.
WAN LED	Flashing	Data is transmitting or receiving on the WAN interface.
	On	Port linked.
	Off	No link.
LAN LED	Flashing	Data is transmitting or receiving on the LAN interface.
	On	Port linked.
	Off	No link.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

1.4 RA-M100 Interface Description

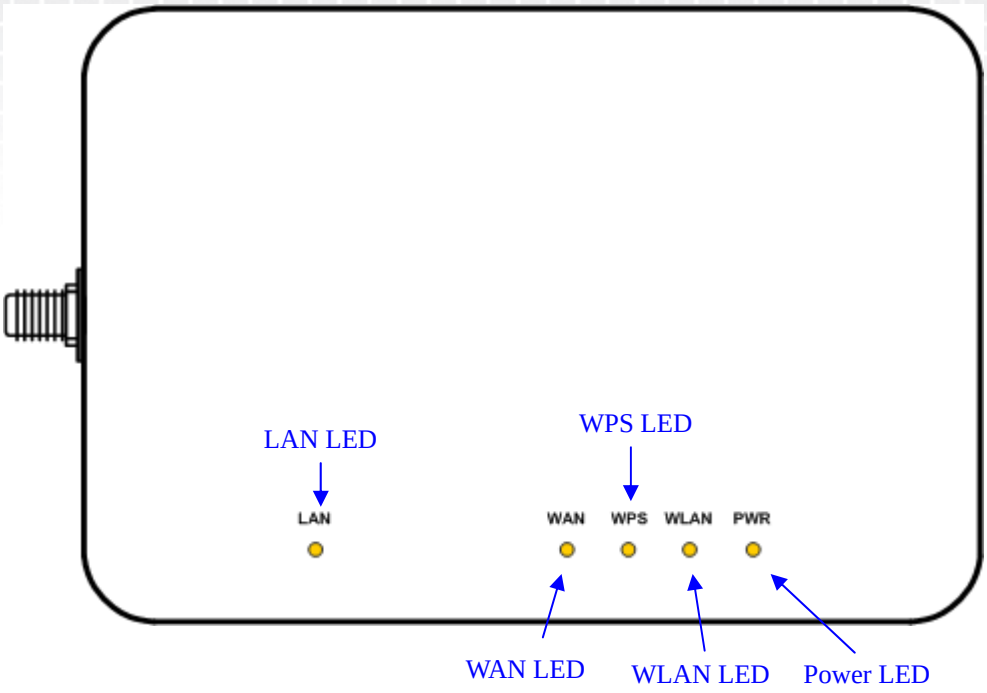


Interfaces	Description
Antenna	The Wireless LAN Antenna. in box
Power	The power jack allows an external DC power supply connection. The external AC to DC adaptor provide adaptive power requirement (2A@5Vdc) to the WLAN Broadband Router.
WAN	The RJ-45 socket allows WAN connection through a Category 5 cable. Support auto-sensing on 10/100M speed and half/ full duplex; comply with IEEE 802.3/ 802.3u respectively.
LAN	The RJ-45 sockets allow LAN connection through Category 5 cables. Support auto-sensing on 10/100M speed and half/ full duplex; comply with IEEE 802.3/ 802.3u respectively.
WPS	Push continually the reset button 5 ~ 10 seconds to enable the WPS feature.
Reset	Push continually the reset button 5 ~ 10 seconds to reset the configuration parameters to factory defaults.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

1.1 RA-M100Plus Panel Description

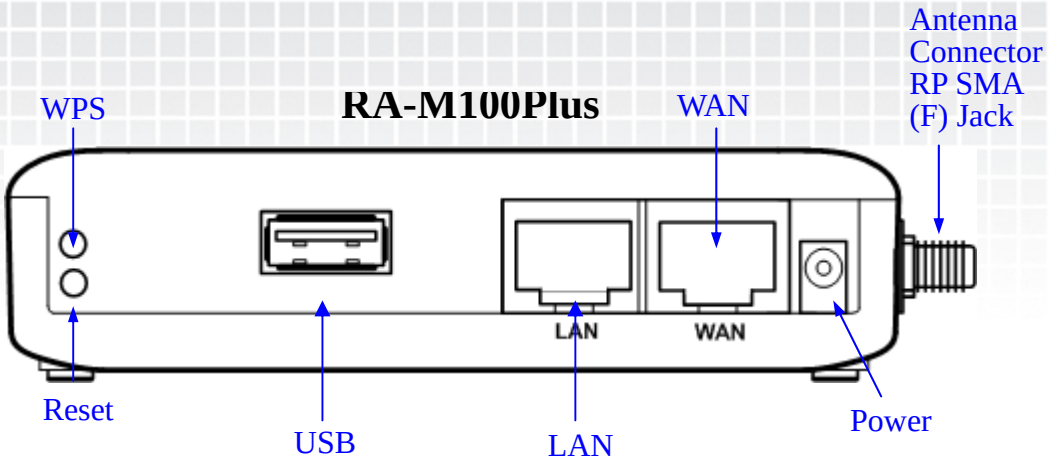
RA-M100Plus



LED Indicator	State	Description
Power LED	On	The WLAN Broadband Router is powered on.
	Off	The WLAN Broadband Router is powered off.
WLAN LED	Flashing	Data is transmitting or receiving on the antenna.
	Off	No data is transmitting or receiving on the antenna.
WPS LED	Flashing	The WPS feature is Enabled.
	Off	The WPS feature is Disabled.
WAN LED	Flashing	Data is transmitting or receiving on the WAN interface.
	On	Port linked.
	Off	No link.
LAN LED	Flashing	Data is transmitting or receiving on the LAN interface.
	On	Port linked.
	Off	No link.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

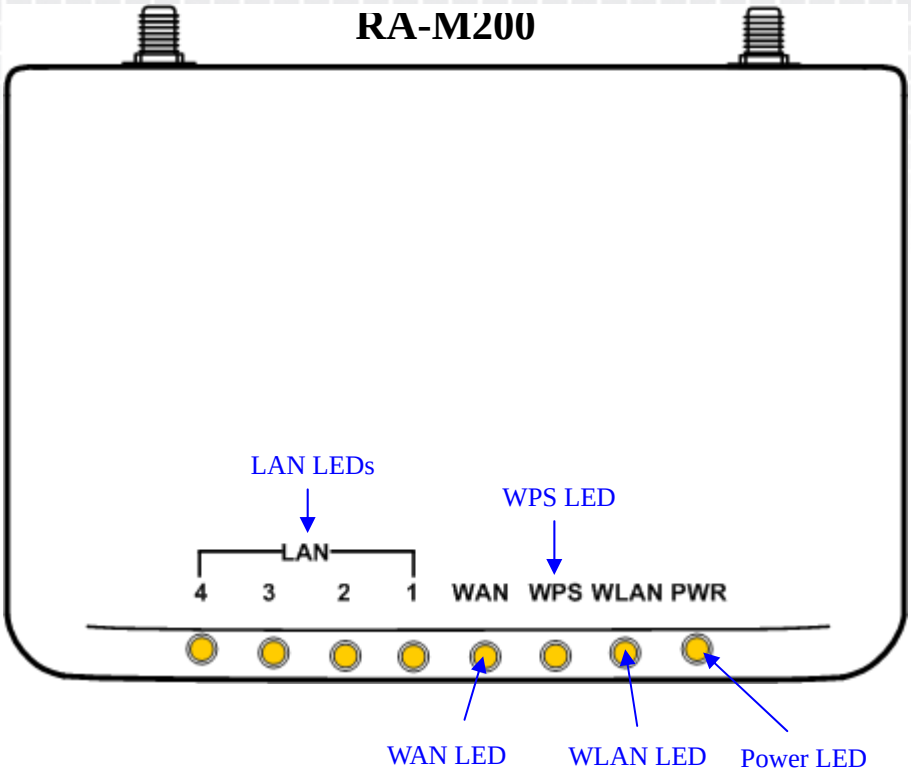
1.2 RA-M100Plus Interface Description



Interfaces	Description
Antenna Connector	One Reverse SMA Jack (Female) for one external 2.4GHz Rubber Duck Antenna.
Power	The power jack allows an external DC power supply connection. The external AC to DC adaptor provide adaptive power requirement (2A@5Vdc) to the WLAN Broadband Router.
WAN	The RJ-45 socket allows WAN connection through a Category 5 cable. Support auto-sensing on 10/100M speed and half/ full duplex; comply with IEEE 802.3/ 802.3u respectively.
LAN	The RJ-45 socket allows LAN connection through Category 5 cables. Support auto-sensing on 10/100M speed and half/ full duplex; comply with IEEE 802.3/ 802.3u respectively.
USB	The USB port allows the connection with: - 3G Dongle for 3G WAN Internet Access 4.36 Which 3.5G devices are compatible with RA-M100Plus? - external storage (Hard Disk or Flash Drive) to support Network File Sharing or FTP Server function.
WPS	Push continually the reset button 5 ~ 10 seconds to enable the WPS feature.
Reset	Push continually the reset button 5 ~ 10 seconds to reset the configuration parameters to factory defaults.

RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

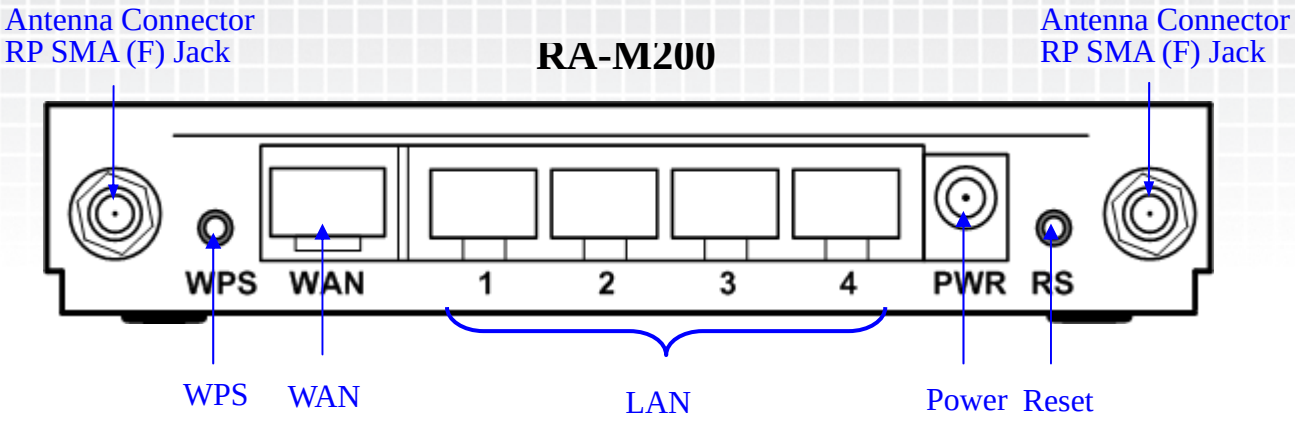
1.3 RA-M200 Panel Description



LED Indicator	State	Description
Power LED	On	The WLAN Broadband Router is powered on.
	Off	The WLAN Broadband Router is powered off.
WLAN LED	Flashing	Data is transmitting or receiving on the antenna.
	Off	No data is transmitting or receiving on the antenna.
WPS LED	Flashing	The WPS feature is Enabled.
	Off	The WPS feature is Disabled.
WAN LED	Flashing	Data is transmitting or receiving on the WAN interface.
	On	Port linked.
	Off	No link.
LAN LED	Flashing	Data is transmitting or receiving on the LAN interface.
	On	Port linked.
	Off	No link.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

1.4 RA-M200 Interface Description



Interfaces	Description
Power	The power jack allows an external DC power supply connection. The external AC to DC adaptor provide adaptive power requirement (1A@5Vdc) to the WLAN Broadband Router.
WAN	The RJ-45 socket allows WAN connection through a Category 5 cable. Support auto-sensing on 10/100M speed and half/ full duplex; comply with IEEE 802.3/ 802.3u respectively.
LAN	The RJ-45 sockets allow LAN connection through Category 5 cables. Support auto-sensing on 10/100M speed and half/ full duplex; comply with IEEE 802.3/ 802.3u respectively.
WPS	Push continually the reset button 5 ~ 10 seconds to enable the WPS feature.
Reset	Push continually the reset button 5 ~ 10 seconds to reset the configuration parameters to factory defaults.
Antenna Connectors	Two Reverse SMA Jacks (Female) for two external 2.4GHz Rubber Duck Antennas.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

2 Installation

2.1 Hardware Installation

Step 1: Place the Wireless LAN Broadband Router to the best optimum transmission location. The best transmission location for your WLAN Broadband Router is usually at the geographic center of your wireless network, with line of sign to all of your mobile stations.

Step 2: Connect the WLAN Broadband Router to your wired network. Connect the Ethernet WAN interface of WLAN Broadband Router by category 5 Ethernet cable to your switch/ hub/ xDSL modem or cable modem. A straight-through Ethernet cable with appropriate cable length is needed.

Step 3: Supply DC power to the WLAN Broadband Router. Use only the AC/DC power adapter supplied with the WLAN Broadband Router; it maybe occur damage by using a different type of power adapter.

The hardware installation finished.

2.2 Software Installation

➢ There are no software drivers, patches or utilities installation needed, but only the configuration setting. Please refer to chapter 3 for software configuration.

Notice: It will take about 50 seconds to complete the boot up sequence after powered on the WLAN Broadband Router; Power LED will be active, and after that the WLAN Activity LED will be flashing to show the WLAN interface is enabled and working now.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

3 Software configuration

There are web based management and configuration functions allowing you to have the jobs done easily.

The WLAN Broadband Router is delivered with the following factory default parameters on the Ethernet LAN interfaces.

Default IP Address: 192.168.10.1

Default IP subnet mask: 255.255.255.0

WEB login User Name: <admin>

WEB login Password: <raytalk>

3.1 Prepare your PC to configure the WLAN Broadband Router

For OS of Microsoft Windows 95/ 98/ Me/XP:

1. Click the ***Start*** button and select ***Settings***, then click ***Control Panel***. The ***Control Panel*** window will appear.
   Note: Windows Me users may not see the Network control panel. If so, *select* **View all Control Panel options** on the left side of the window
2. Move mouse and double-click the right button on ***Network*** icon. The ***Network*** window will appear.
3. Check the installed list of ***Network Components***. If TCP/IP is not installed, click the ***Add*** button to install it; otherwise go to step 6.
4. Select ***Protocol*** in the ***Network Component Type*** dialog box and click ***Add*** button.
5. Select ***TCP/IP*** in ***Microsoft*** of ***Select Network Protocol*** dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to ***Network*** dialog box after the TCP/IP installation.
6. Select ***TCP/IP*** and click the ***properties*** button on the ***Network*** dialog box.
7. Select ***Specify an IP address*** and type in values as following example.
   - ✓ IP Address: **192.168.10.1**, any IP address within 192.168.10.1 to

 Copyright © RayTalk Industries. Tutti i diritti riservati.

192.168.10.253 is good to connect the Wireless LAN Access Point.

- ✓ IP Subnet Mask: **255.255.255.0**

8. Click OK and reboot your PC after completes the IP parameters setting.

For OS of Microsoft Windows 2000, XP:

1. Click the ***Start*** button and select ***Settings***, then click ***Control Panel***. The ***Control Panel*** window will appear.
2. Move mouse and double-click the right button on ***Network and Dial-up Connections*** icon. Move mouse and double-click the ***Local Area Connection*** icon. The ***Local Area Connection*** window will appear. Click ***Properties*** button in the ***Local Area Connection*** window.
3. Check the installed list of ***Network Components***. If TCP/IP is not installed, click the ***Add*** button to install it; otherwise go to step 6.
4. Select ***Protocol*** in the ***Network Component Type*** dialog box and click ***Add*** button.
5. Select ***TCP/IP*** in ***Microsoft*** of ***Select Network Protocol*** dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to ***Network*** dialog box after the TCP/IP installation.
6. Select ***TCP/IP*** and click the ***properties*** button on the ***Network*** dialog box.
7. Select ***Specify an IP address*** and type in values as following example.
   - ✓ IP Address: **192.168.10.1**, any IP address within 192.168.10.1 to 192.168.10.253 is good to connect the Wireless LAN Access Point.
   - ✓ IP Subnet Mask: **255.255.255.0**
8. Click OK to completes the IP parameters setting.

For OS of Microsoft Windows NT:

1. Click the ***Start*** button and select ***Settings***, then click ***Control Panel***. The ***Control Panel*** window will appear.
2. Move mouse and double-click the right button on ***Network*** icon. The ***Network*** window will appear. Click ***Protocol*** tab from the ***Network*** window.
3. Check the installed list of ***Network Protocol*** window. If TCP/IP is not installed, click the ***Add*** button to install it; otherwise go to step 6.
4. Select ***Protocol*** in the ***Network Component Type*** dialog box and click ***Add*** button.
5. Select ***TCP/IP*** in ***Microsoft*** of ***Select Network Protocol*** dialog box then click OK

 Copyright © RayTalk Industries. Tutti i diritti riservati.

button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to ***Network*** dialog box after the TCP/IP installation.

6. Select ***TCP/IP*** and click the ***properties*** button on the ***Network*** dialog box.
7. Select ***Specify an IP address*** and type in values as following example.
   - ✓ IP Address: **192.168.10.1**, any IP address within 192.168.10.1 to 192.168.10.253 is good to connect the Wireless LAN Access Point.
   - ✓ IP Subnet Mask: **255.255.255.0**
8. Click OK to complete the IP parameters setting.

For OS of Microsoft Windows Vista:

1. Click the ***Start*** button and select ***Settings***, then click ***Control Panel***. The Control ***Panel*** window will appear.
2. Move mouse and double-click the right button on ***Network Connections*** item. The ***Network Connections*** window will appear. Double click ***Local Area Connection*** icon, then ***User Account Control*** window shown. Right click ***Continue*** button to set properties.
3. In ***Local Area Connection Properties*** window, Choose ***Networking*** tab, move mouse and click ***Internet Protocol Version 4 (TCP/IPv4)***, then click ***Properties*** button.
4. Move mouse and click ***General*** tab, Select ***Specify an IP address*** and type in values as following example.
   - ✓ IP Address: **192.168.10.1**, any IP address within 192.168.10.1 to 192.168.10.253 is good to connect the Wireless LAN Access Point.
   - ✓ IP Subnet Mask: **255.255.255.0**
5. Click OK to complete the IP parameters setting.

3.2 Connect to the WLAN Broadband Router

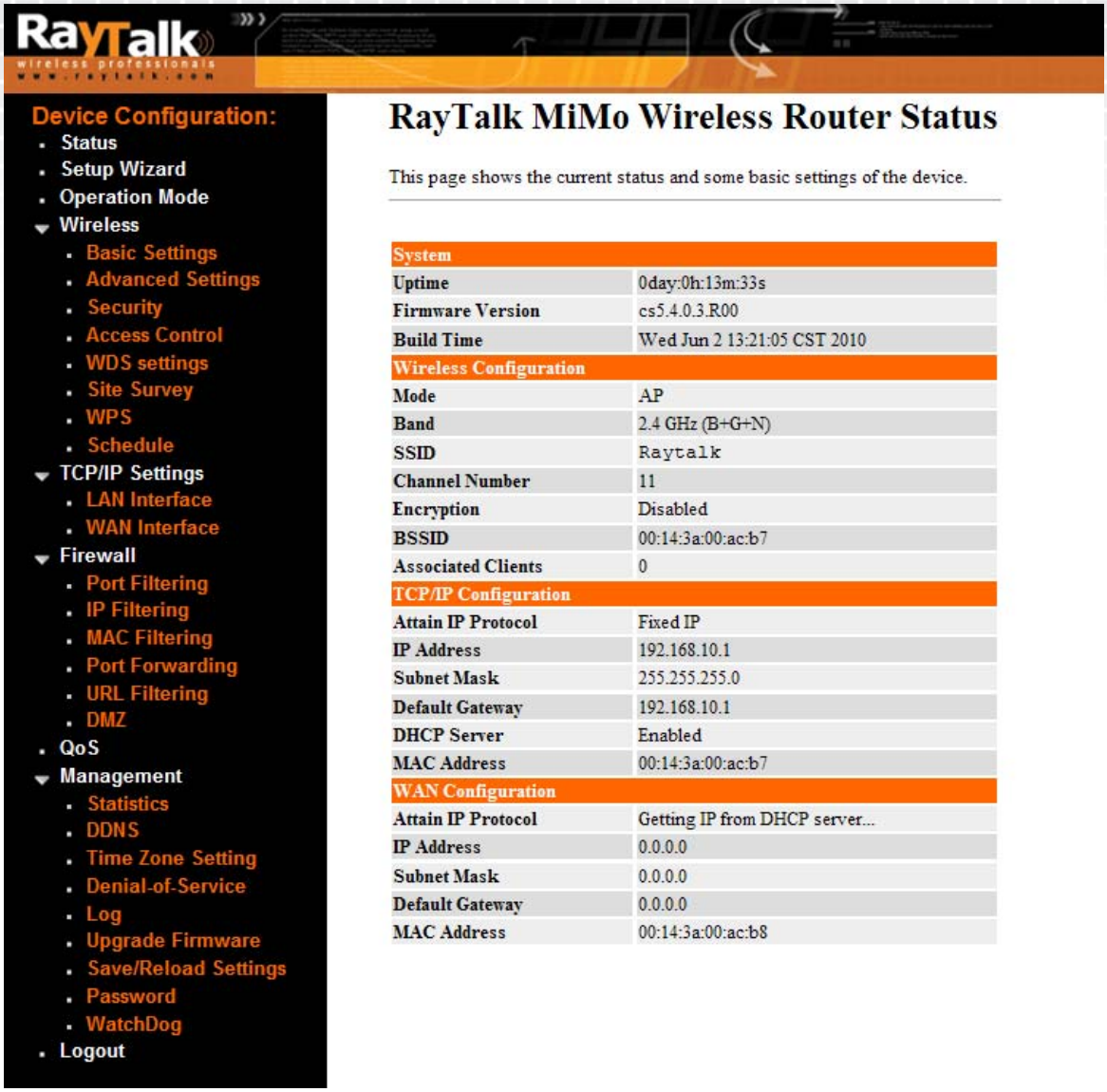
Open a WEB browser, i.e. Microsoft Internet Explore 6.1 SP1 or above, then enter 192.168.1.254 on the URL to connect the WLAN Broadband Router.

3.3 Management and configuration on the WLAN Broadband Router

3.3.1 Status

This page shows the current status and some basic settings of the device, includes system, wireless, Ethernet LAN and WAN configuration information.

RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.



Item	Description
System	
Uptime	It shows the duration since WLAN Broadband Router is powered on.
Firmware version	It shows the firmware version of WLAN Broadband Router.
Build time	It shows the Build-up time of firmware
Wireless configuration	
Mode	It shows wireless operation mode

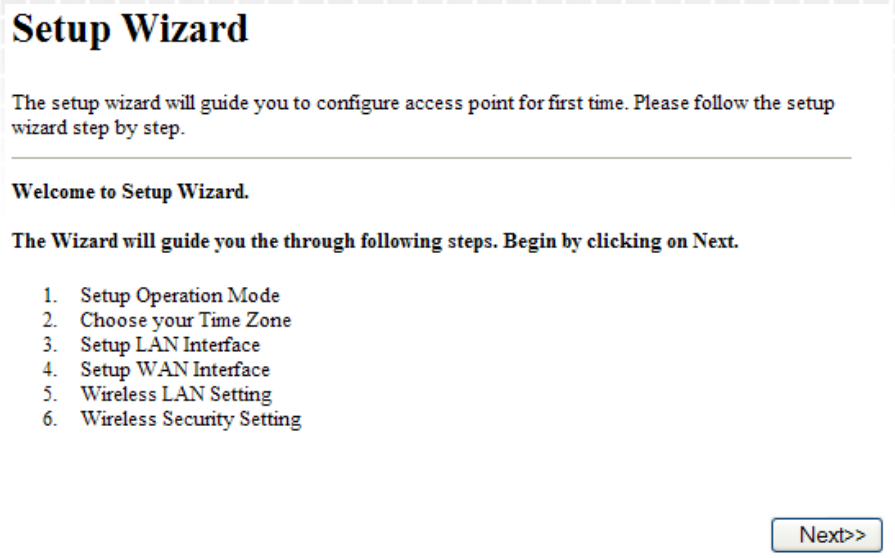
 Copyright © RayTalk Industries. Tutti i diritti riservati.

Band	It shows the current wireless operating frequency.
SSID	It shows the SSID of this WLAN Broadband Router. The SSID is the unique name of WLAN Broadband Router and shared among its service area, so all devices attempts to join the same wireless network can identify it.
Channel Number	It shows the wireless channel connected currently.
Encryption	It shows the status of encryption function.
BSSID	It shows the BSSID address of the WLAN Broadband Router. BSSID is a six-byte address.
Associated Clients	It shows the number of connected clients (or stations, PCs).
TCP/IP configuration	
Attain IP Protocol	It shows type of connection.
IP Address	It shows the IP address of LAN interfaces of WLAN Broadband Router.
Subnet Mask	It shows the IP subnet mask of LAN interfaces of WLAN Broadband Router.
Default Gateway	It shows the default gateway setting for LAN interfaces outgoing data packets.
DHCP Server	It shows the DHCP server is enabled or not.
MAC Address	It shows the MAC address of LAN interfaces of WLAN Broadband Router.
WAN configuration	
Attain IP Protocol	It shows how the WLAN Broadband Router gets the IP address. The IP address can be set manually to a fixed one or set dynamically by DHCP server or attain IP by PPPoE / PPTP connection.
IP Address	It shows the IP address of WAN interface of WLAN Broadband Router.
Subnet Mask	It shows the IP subnet mask of WAN interface of WLAN Broadband Router.
Default Gateway	It shows the default gateway setting for WAN interface outgoing data packets.
MAC Address	It shows the MAC address of WAN interface of WLAN Broadband Router.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

3.3.2 Setup Wizard

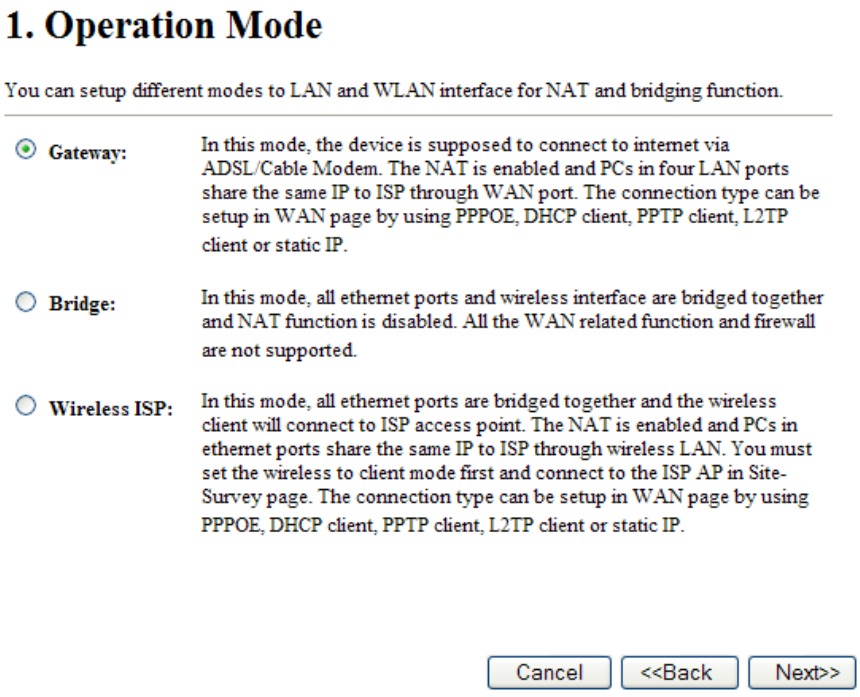
This page guides you to configure wireless broadband router for first time


Setup Wizard
The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.
Welcome to Setup Wizard.
The Wizard will guide you the through following steps. Begin by clicking on Next.
1. Setup Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Interface
5. Wireless LAN Setting
6. Wireless Security Setting
Next>>

Note: Gateway mode is only choice for GSM3G WAN connection for RA-M100Plus.

I Operation Mode

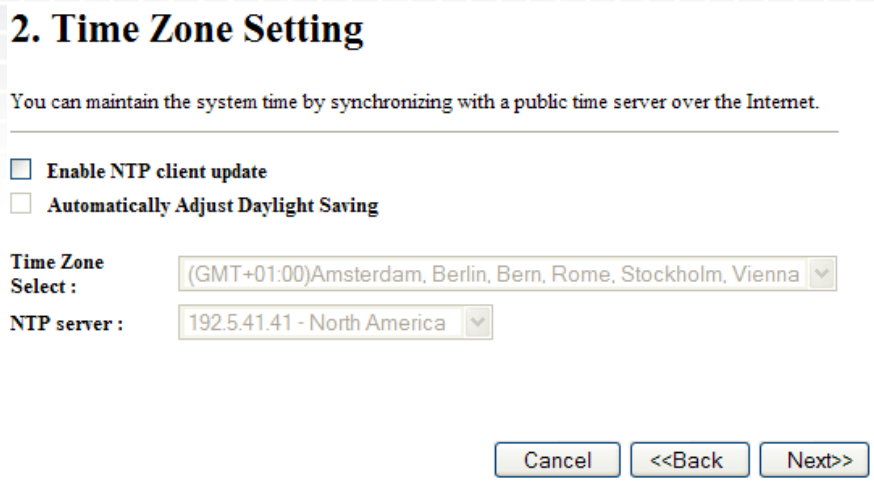
This page followed by Setup Wizard page to define the operation mode.


1. Operation Mode
You can setup different modes to LAN and WLAN interface for NAT and bridging function.
Gateway: In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.
Bridge: In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
Wireless ISP: In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.
Cancel
<<Back
Next>>

 Copyright © RayTalk Industries. Tutti i diritti riservati.

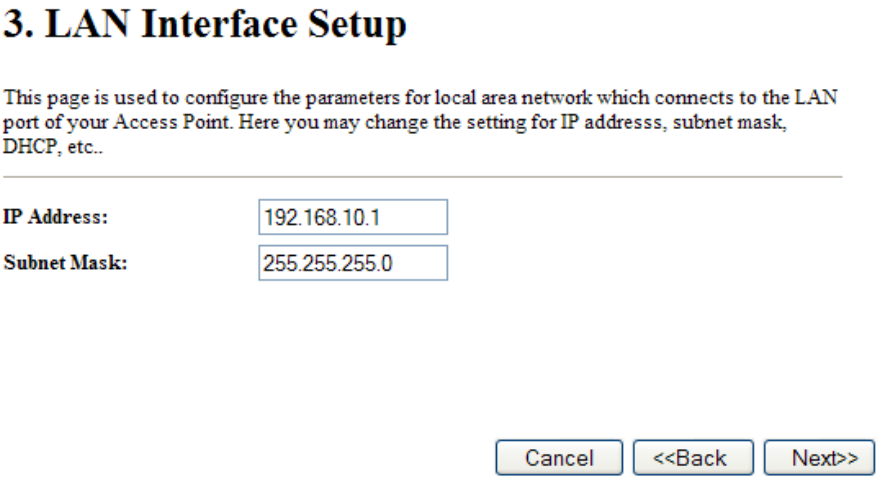
II Time Zone Setting

This page is used to enable and configure NTP client


2. Time Zone Setting
You can maintain the system time by synchronizing with a public time server over the Internet.
Enable NTP client update
Automatically Adjust Daylight Saving
Time Zone Select :
(GMT+01:00)Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
NTP server :
192.5.41.41 - North America
Cancel
<<Back
Next>>

III LAN Interface Setup

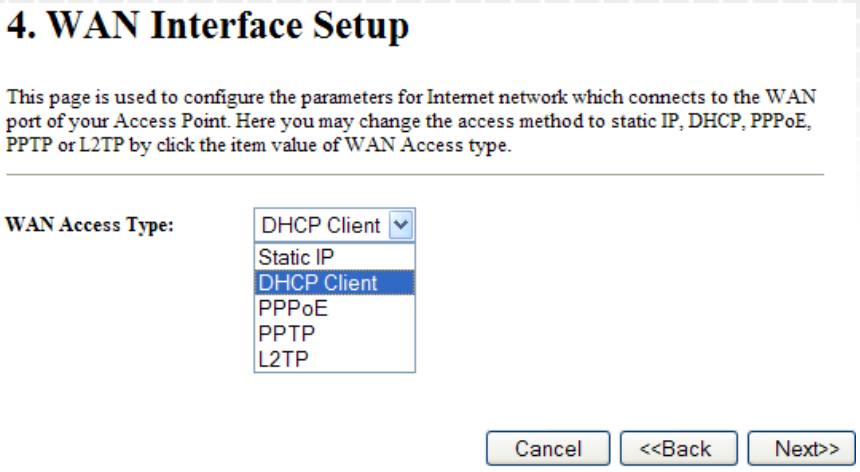
This page is used to configure local area network IP address and subnet mask


3. LAN Interface Setup
This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..
IP Address:
192.168.10.1
Subnet Mask:
255.255.255.0
Cancel
<<Back
Next>>

 Copyright © RayTalk Industries. Tutti i diritti riservati.

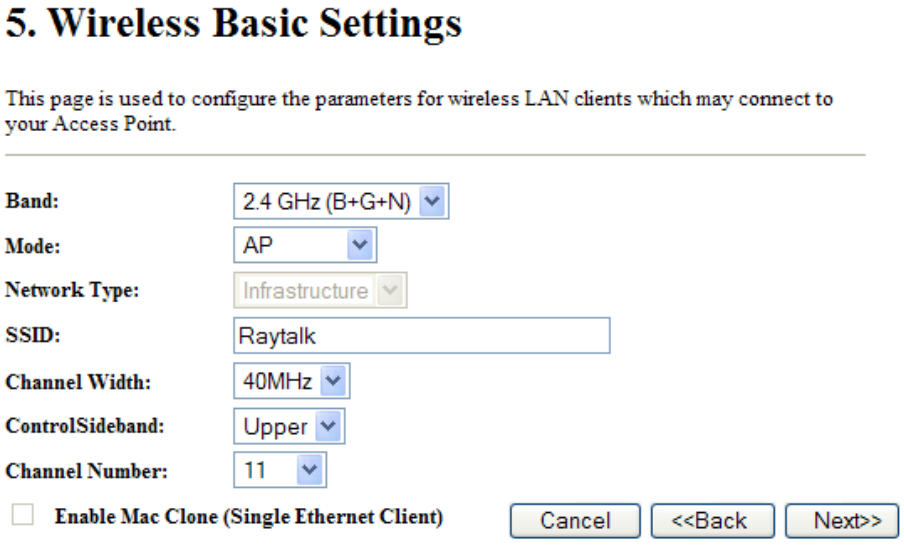
IV WAN Interface Setup

This page is used to configure WAN access type


4. WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.
WAN Access Type:
DHCP Client
Static IP
DHCP Client
PPPoE
PPTP
L2TP
Cancel
<<Back
Next>>

V Wireless Basic Settings

This page is used to configure basic wireless parameters like Band, Mode, Network Type SSID, Channel Number, Enable Mac Clone (Single Ethernet Client).



 Copyright © RayTalk Industries. Tutti i diritti riservati.

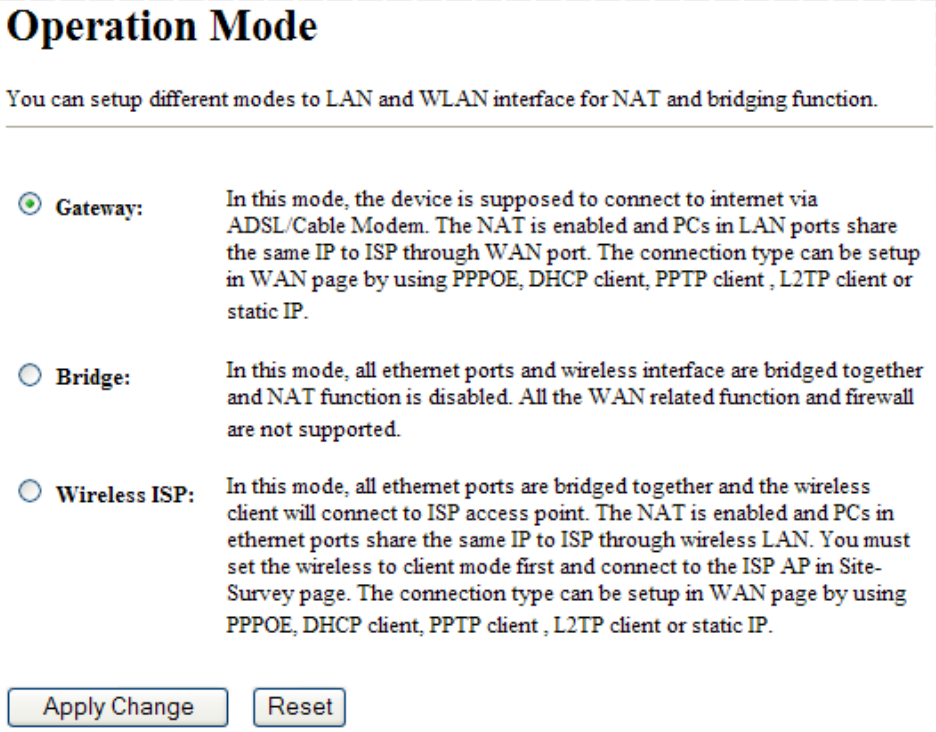
VI Wireless Security Setup

This page is used to configure wireless security

 Copyright © RayTalk Industries. Tutti i diritti riservati.

3.3.3 Operation Mode

This page is used to configure which mode wireless broadband router acts

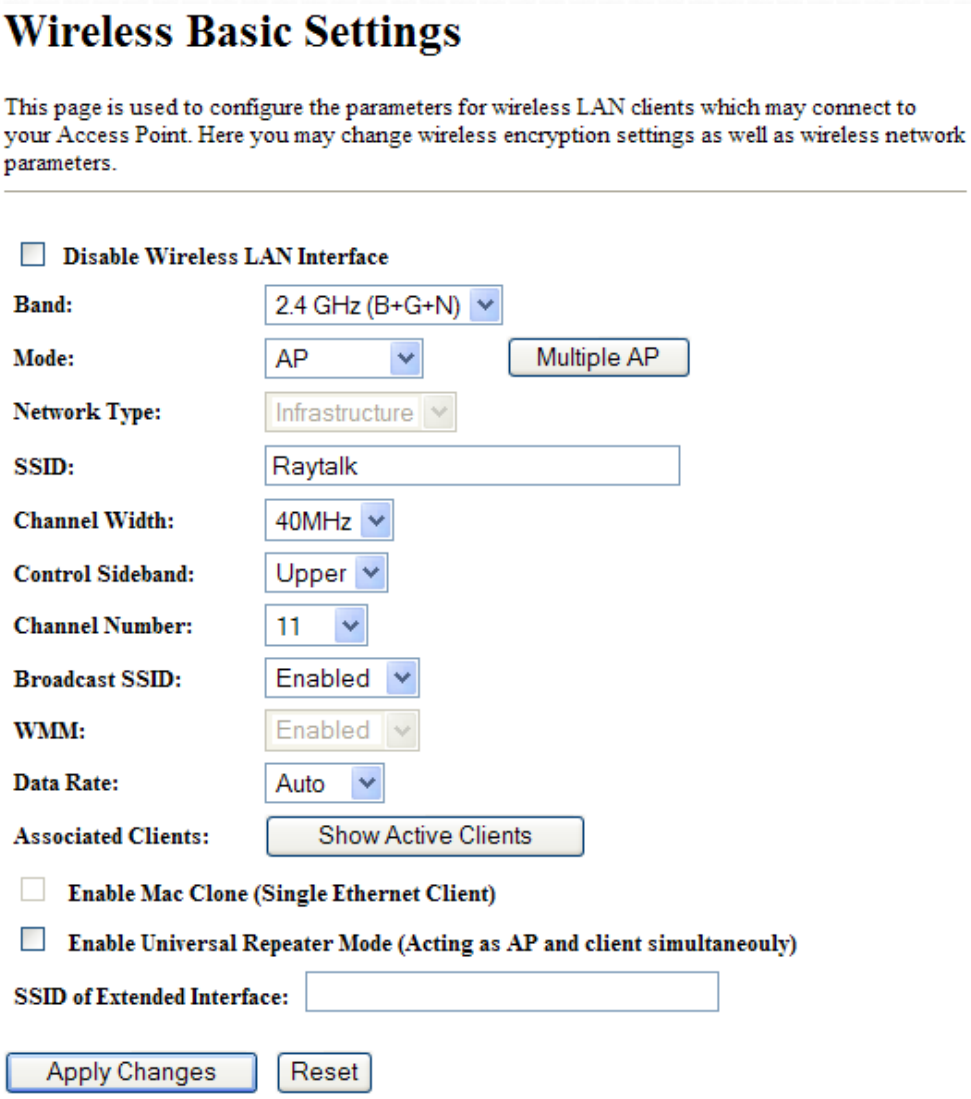

Operation Mode
You can setup different modes to LAN and WLAN interface for NAT and bridging function.
Gateway:
In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client , L2TP client or static IP.
Bridge:
In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
Wireless ISP:
In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client , L2TP client or static IP.
Apply Change
Reset

Item	Description
Gateway	Traditional gateway configuration. It always connects internet via ADSL/Cable Modem. LAN interface, WAN interface, Wireless interface, NAT and Firewall modules are applied to this mode. Gateway mode is only choice for GSM3G WAN connection for RA-M100Plus.
Bridge	Each interface (LAN, WAN and Wireless) regards as bridge. NAT, Firewall and all router's functions are not supported
Wireless ISP	Switch Wireless interface to WAN port and all Ethernet ports in bridge mode. Wireless interface can do all router's functions
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

3.3.4 Wireless - Basic Settings

This page is used to configure the parameters for wireless LAN clients that may connect to your Broadband Router. Here you may change wireless encryption settings as well as wireless network parameters.



Item	Description
Disable Wireless LAN Interface	Click on to disable the wireless LAN data transmission.
Band	Click to select 2.4GHz(B) / 2.4GHz(G) / 2.4GHz(N) 2.4GHz(B+G)/ 2.4GHz(G+N) / 2.4GHz(B+G+N)
Mode	Click to select the WLAN AP / Client / WDS / AP+WDS wireless mode.

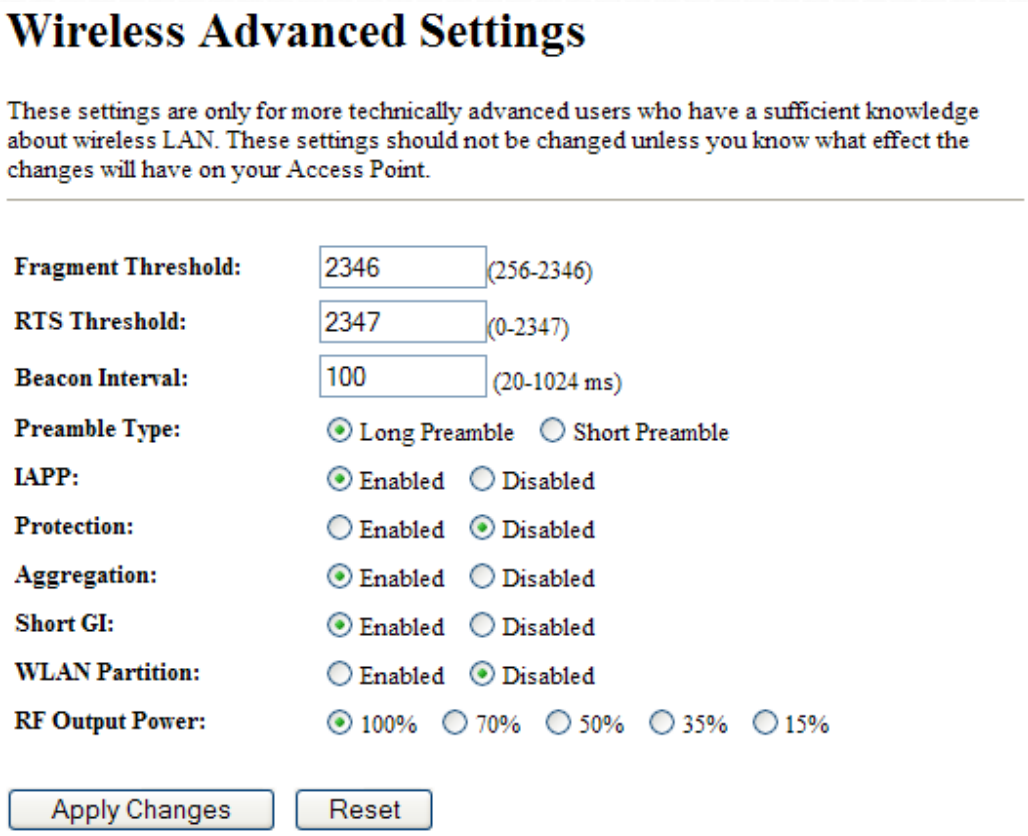
 Copyright © RayTalk Industries. Tutti i diritti riservati.

	Note: RA-M100Plus and u2.3.0.3.R00 firmware support Mesh and AP+Mesh features. 4.22 What is Universal Plug and Play (uPNP)?
Network Type	While ***Mode*** is selected to be **Client**. Click to select the network type infrastructure or Ad hoc.
SSID	It is the wireless network name. The SSID can be 32 bytes long.
Channel Width	Select the operating channel width 20 MHz or 40 MHz. **[N band only]**
Control Sideband	Select the Sideband with Upper or Lower for channel width 40MHz. **[N band only]**
Channel Number	Select the wireless communication channel from pull-down menu.
Broadcast SSID	Click to enable or disable the SSID broadcast function. Refer to 4.14 What is SSID Broadcast?
WMM	Click Enabled/Disable*d* to init WMM feature.
Data Rate	Select the transmission data rate from pull-down menu. Data rate can be auto-select, 1M to 54Mbps or MCS. Refer to 4.32 What is Modulation Coding Schemes (MCS)?
Associated Clients	Click the ***Show Active Clients*** button to open Active Wireless Client Table that shows the MAC address, transmit-packet, receive-packet and transmission-rate for each associated wireless client.
Enable Mac Clone (Single Ethernet Client)	Take Laptop NIC MAC address as wireless client MAC address. **[Client Mode only]**
Enable Universal Repeater Mode	Click to enable Universal Repeater Mode
SSID of Extended Interface	Assign SSID when enables Universal Repeater Mode.
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

3.3.5 Wireless - Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your WLAN Broadband Router.


Wireless Advanced Settings
These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.
Fragment Threshold: 2346 (256-2346)
RTS Threshold: 2347 (0-2347)
Beacon Interval: 100 (20-1024 ms)
Preamble Type: Long Preamble Short Preamble
IAPP: Enabled Disabled
Protection: Enabled Disabled
Aggregation: Enabled Disabled
Short GI: Enabled Disabled
WLAN Partition: Enabled Disabled
RF Output Power: 100% 70% 50% 35% 15%
Apply Changes
Reset

Item	Description
Fragment Threshold	Set the data packet fragmentation threshold, value can be written between 256 and 2346 bytes. Refer to 4.10 What is Fragment Threshold?
RTS Threshold	Set the RTS Threshold, value can be written between 0 and 2347 bytes. Refer to 4.11 What is RTS(Request To Send) Threshold?
Beacon Interval	Set the Beacon Interval, value can be written between 20 and 1024 ms. Refer to 4.12 What is Beacon Interval?
Preamble Type	Click to select the ***Long Preamble*** or ***Short Preamble*** support on the wireless data packet

 Copyright © RayTalk Industries. Tutti i diritti riservati.

	transmission. Refer to 4.13 What is Preamble Type?
IAPP	Click to enable or disable the IAPP function. Refer to 4.20 What is Inter-Access Point Protocol(IAPP)?
Protection	Protect 802.11n user priority.
Aggregation	Click to enable or disable the Aggregation function. Refer to 4.33 What is Aggregation?
Short GI	Click to enable or disable the short Guard Intervals function. Refer to 4.34 What is Guard Intervals (GI)?
WLAN Partition	Click to enable or disable that prevents associated wireless clients from communication with each other.
RF Output Power	To adjust transmission power level.
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

3.3.6 Wireless - Security Setup

This page allows you setup the wireless security. Turn on WEP, WPA, WPA2 by using encryption keys could prevent any unauthorized access to your wireless network.

Wireless Security Setup
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.
Select SSID:
Root AP - Raytalk
Apply Changes
Reset
Encryption:
Disable
802.1x Authentication:

Item	Description
Select SSID	Select the SSID from multiple APs.
Encryption	Select the encryption supported over wireless access. The encryption method can be None, WEP, WPA, WPA2 or WPA-Mixed. Refer to 4.9 What is WEP? 4.15 What is Wi-Fi Protected Access (WPA)? 4.16 What is WPA2?
Use 802.1x Authentication	While Encryption is selected to be WEP. Click the check box to enable IEEE 802.1x authentication function. Refer to 4.17 What is 802.1x Authentication?
Authentication Type	Click to select the authentication type in ***Open System***, ***Shared Key*** or ***Auto*** selection.
Key Length	Select the WEP shared secret key length from pull-down menu. The length can be chose between 64-bit and 128-bit (known as “WEP2”) keys. The WEP key is composed of initialization vector (24 bits) and secret key (40-bit or 104-bit).
Key Format	Select the WEP shared secret key format from

RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

	pull-down menu. The format can be chose between plant text (ASCII) and hexadecimal (HEX) code.
Encryption Key	Secret key of WEP security encryption function.
WPA Authentication Mode	While Encryption is selected to be WPA. Click to select the WPA Authentication Mode with Enterprise (RADIUS) or Personal (Pre-Shared Key). Refer to 4.15 What is Wi-Fi Protected Access (WPA)?
WPA Cipher Suite	Select the Cipher Suite for WPA encryption. 4.18 What is Temporal Key Integrity Protocol (TKIP)? 4.19 What is Advanced Encryption Standard (AES)?
WPA2 Cipher Suite	Select the Cipher Suite for WPA2 encryption.
Pre-Shared Key Format	While Encryption is selected to be WPA. Select the Pre-shared key format from the pull-down menu. The format can be Passphrase or Hex (64 characters). **[WPA, Personal(Pre-Shared Key) only]**
Pre-Shared Key	Fill in the key value. [WPA, Personal(Pre-Shared Key) only]
Enable Pre-Authentication	Click to enable Pre-Authentication. [WPA2/WPA2 Mixed only, Enterprise only]
Authentication RADIUS Server	Set the IP address, port and login password information of authentication RADIUS sever.
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

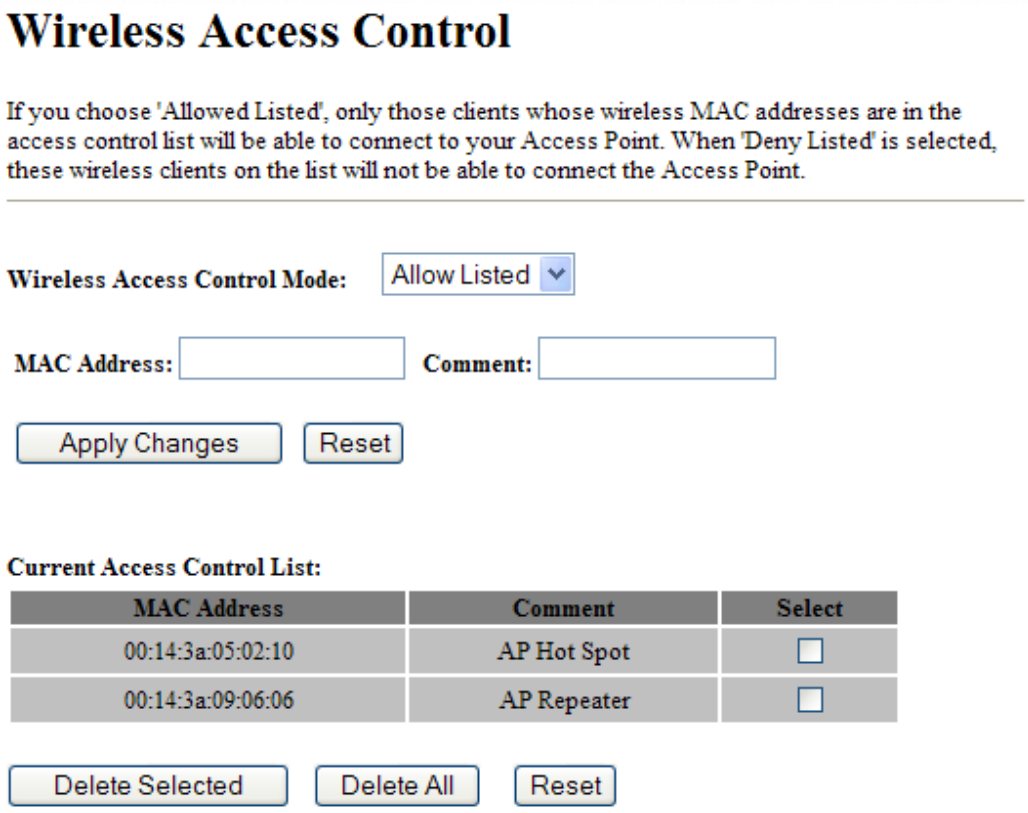
WEP encryption key (secret key) length:

Length / Format	64-bit	128-bit
ASCII	5 characters	13 characters
HEX	10 hexadecimal codes	26 hexadecimal codes

 Copyright © RayTalk Industries. Tutti i diritti riservati.

3.3.7 Wireless - Access Control

If you enable wireless access control, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When this option is enabled, no wireless clients will be able to connect if the list contains no entries.


Wireless Access Control
If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.
Wireless Access Control Mode:
Allow Listed
MAC Address:
Comment:
Apply Changes
Reset
Current Access Control List:
MAC Address
Comment
Select
00:14:3a:05:02:10
AP Hot Spot
00:14:3a:09:06:06
AP Repeater
Delete Selected
Delete All
Reset

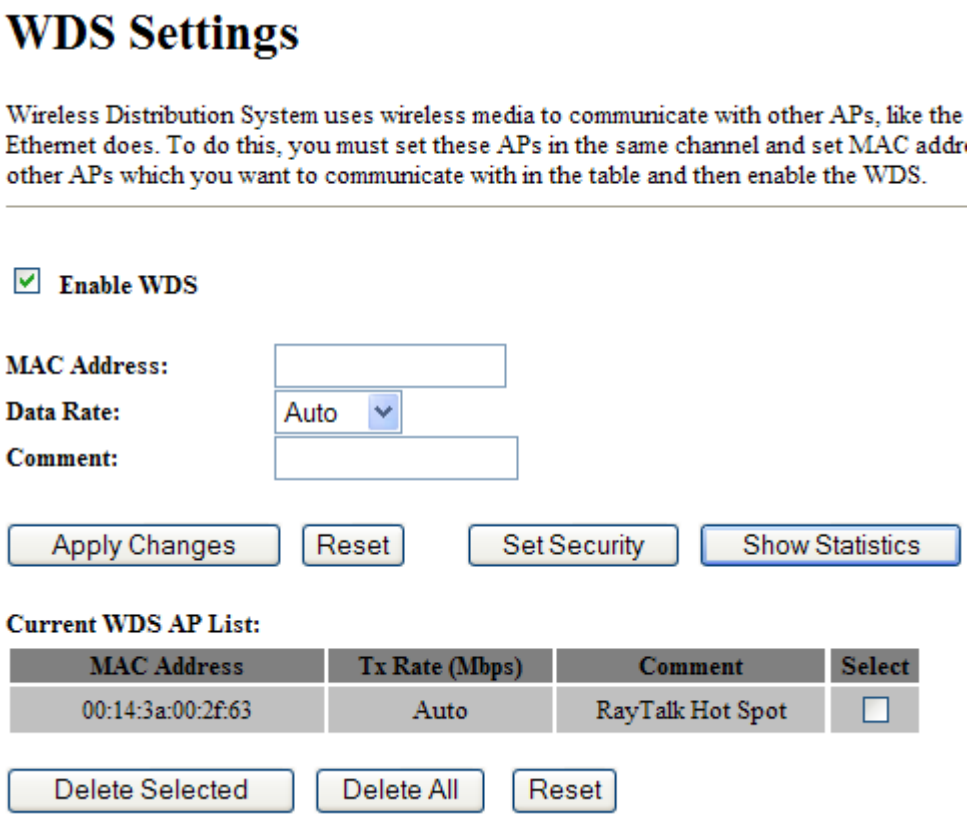
Item	Description
Wireless Access Control Mode	Click the ***Disabled***, ***Allow Listed*** or ***Deny Listed*** of drop down menu choose wireless access control mode. This is a security control function; only those clients registered in the access control list can link to this WLAN Broadband Router.
MAC Address	Fill in the MAC address of client to register this WLAN Broadband Router access capability.
Comment	Fill in the comment tag for the registered client.
Apply Changes	Click the ***Apply Changes*** button to register the client to new configuration setting.

RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Current Access Control List	It shows the registered clients that are allowed to link to this WLAN Broadband Router.
Delete Selected	Click to delete the selected clients that will be access right removed from this WLAN Broadband Router.
Delete All	Click to delete all the registered clients from the access allowed list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

3.3.8 WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other AP that you want to communicate with in the table and then enable the WDS.



RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

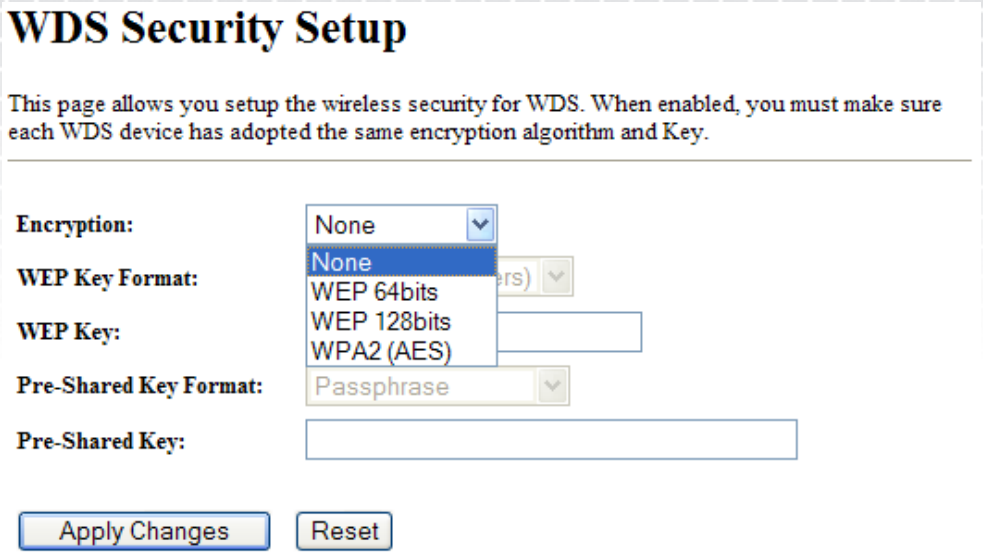
Item	Description
Enable WDS	Click the check box to enable wireless distribution system. Refer to 4.21 What is Wireless Distribution System (WDS)?
MAC Address	Fill in the MAC address of AP to register the wireless distribution system access capability.
Data Rate	Select the transmission data rate from pull-down menu. Data rate can be auto-select, 1M to 54Mbps or MCS.
Comment	Fill in the comment tag for the registered AP.
Apply Changes	Click the ***Apply Changes*** button to register the AP to new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Set Security	Click button to configure wireless security like ***WEP(64bits), WEP(128bits), WPA(TKIP), WPA2(AES)*** or ***None***
Show Statistics	It shows the TX, RX packets, rate statistics
Delete Selected	Click to delete the selected clients that will be removed from the wireless distribution system.
Delete All	Click to delete all the registered APs from the wireless distribution system allowed list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

I WDS Security Setup

Requirement: Set [Wireless]->[Basic Settings]->[Mode]->AP+WDS

This page is used to configure the wireless security between APs. Refer to 3.3.6 Wireless Security Setup.

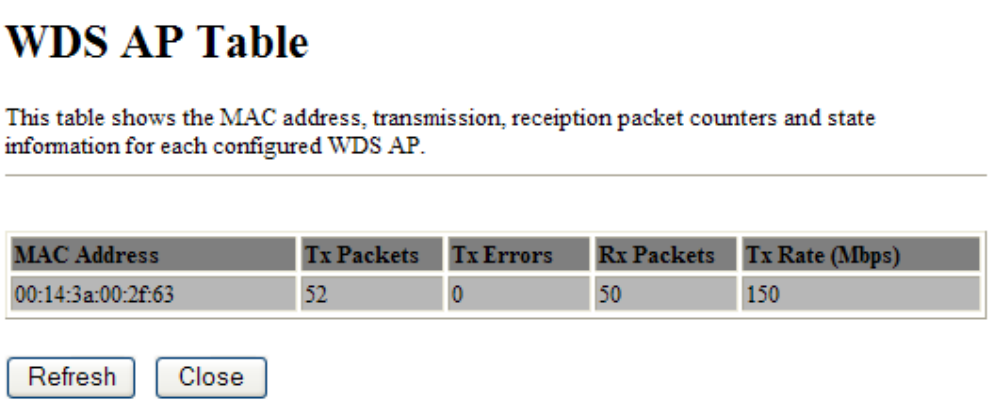
RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.



Screen snapshot – WDS Security Setup

II WDS AP Table

This page is used to show WDS statistics



Item	Description
MAC Address	It shows the MAC Address within WDS.
Tx Packets	It shows the statistic count of sent packets on the wireless LAN interface.
Tx Errors	It shows the statistic count of error sent packets on the Wireless LAN interface.
Rx Packets	It shows the statistic count of received packets on the wireless LAN interface.

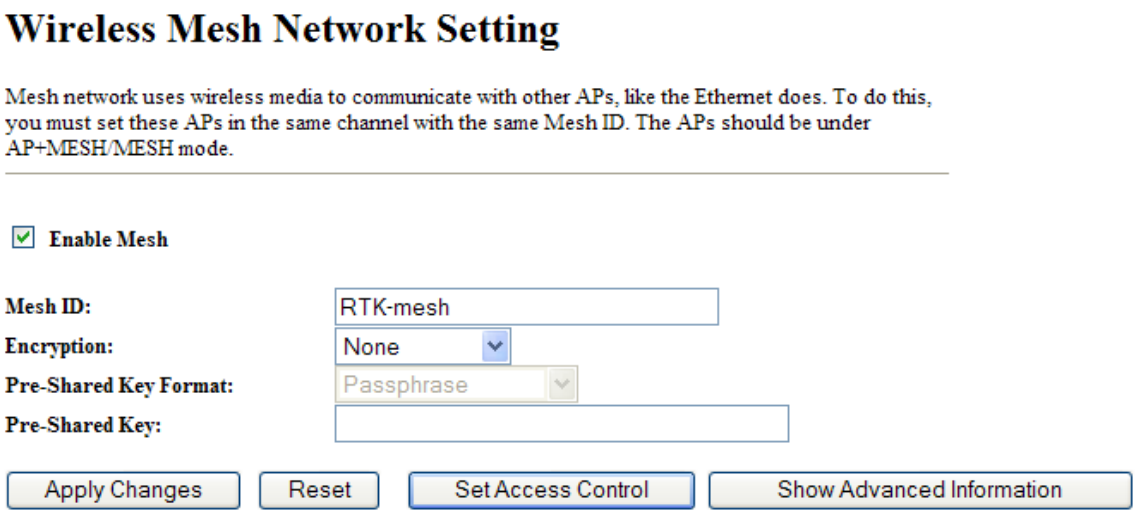
 Copyright © RayTalk Industries. Tutti i diritti riservati.

Tx Rare (Mbps)	It shows the wireless link rate within WDS.
Refresh	Click to refresh the statistic counters on the screen.
Close	Click to close the current window.

3.3.9 Wireless Mesh Network Settings (only RA-M100Plus)

Mesh network uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel with the same Mesh ID. The APs should be under AP+MESH/MESH mode.

This feature is available on RA-M100Plus or firmware u2.3.0.3.R00.


Wireless Mesh Network Setting
Mesh network uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel with the same Mesh ID. The APs should be under AP+MESH/MESH mode.
Enable Mesh
Mesh ID:
RTK-mesh
Encryption:
None
Pre-Shared Key Format:
Passphrase
Pre-Shared Key:
Apply Changes
Reset
Set Access Control
Show Advanced Information

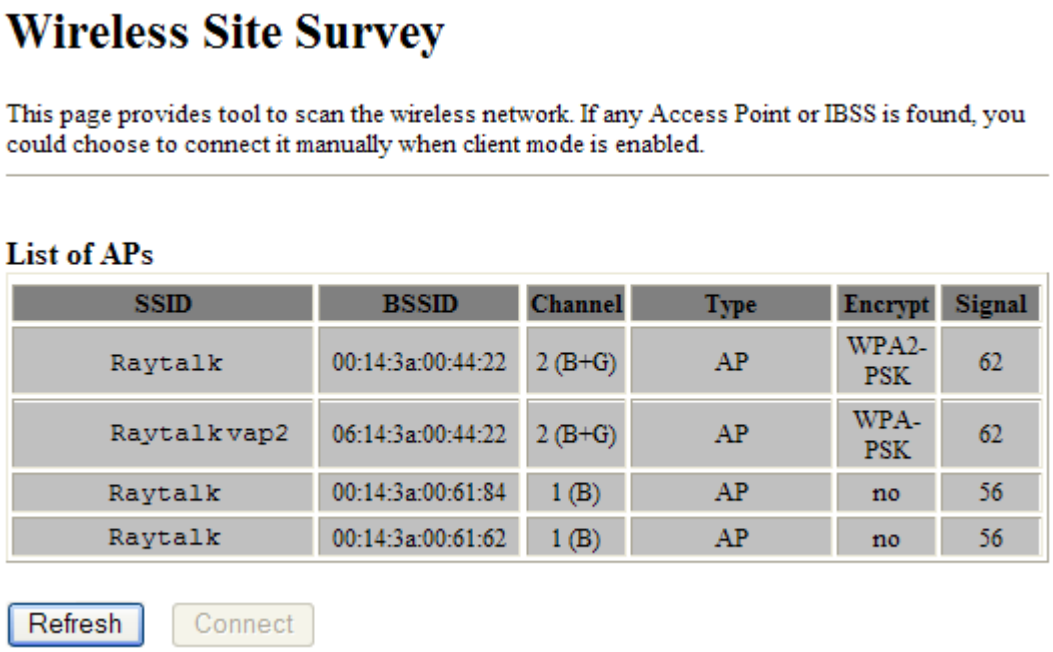
Item	Description
Enable Mesh	Click the check box to enable Mesh connection to other Mesh Node devices. 4.35 What is Mesh protocol?
Encryption	Select the encryption supported over wireless access. The encryption method can be None or WPA2 (AES). Refer to 4.16 What is WPA2?
Apply Changes	Click the ***Apply Changes*** button to register the AP to new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Set Access Control	If you choose 'Allowed Listed', only those mesh nodes whose wireless MAC addresses are in the access control

RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

	list will be able to connect to Mesh network. When 'Deny Listed' is selected, those mesh nodes in the list will not be able to create connections.
Show Advanced Information	These information is only for more technically advanced users who have a sufficient knowledge about wireless mesh network.

3.3.10 Site Survey

This page is used to view or configure other APs near yours.



Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

List of APs

SSID	BSSID	Channel	Type	Encrypt	Signal
Raytalk	00:14:3a:00:44:22	2 (B+G)	AP	WPA2-PSK	62
Raytalkvap2	06:14:3a:00:44:22	2 (B+G)	AP	WPA-PSK	62
Raytalk	00:14:3a:00:61:84	1 (B)	AP	no	56
Raytalk	00:14:3a:00:61:62	1 (B)	AP	no	56

Refresh Connect

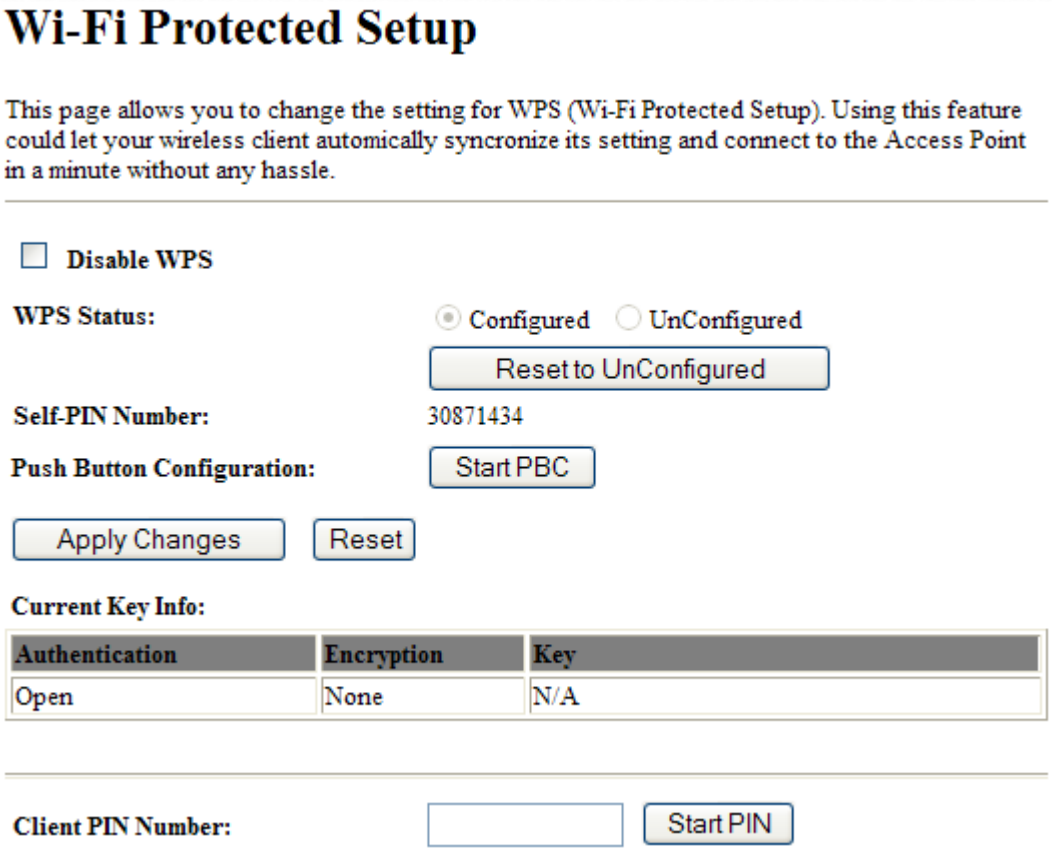
Item	Description
SSID	It shows the SSID of AP.
BSSID	It shows BSSID of AP.
Channel	It show the current channel of AP occupied.
Type	It show which type AP acts.
Encrypt	It shows the encryption status.
Signal	It shows the power level of current AP.
Select (Client Only)	Click to select AP or client you'd like to connect.
Refresh	Click the ***Refresh*** button to re-scan site survey on the screen.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

Connect	Click the ***Connect*** button to establish connection.

3.3.11 WPS

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically synchronize its setting and connect to the Access Point in a minute without any hassle.



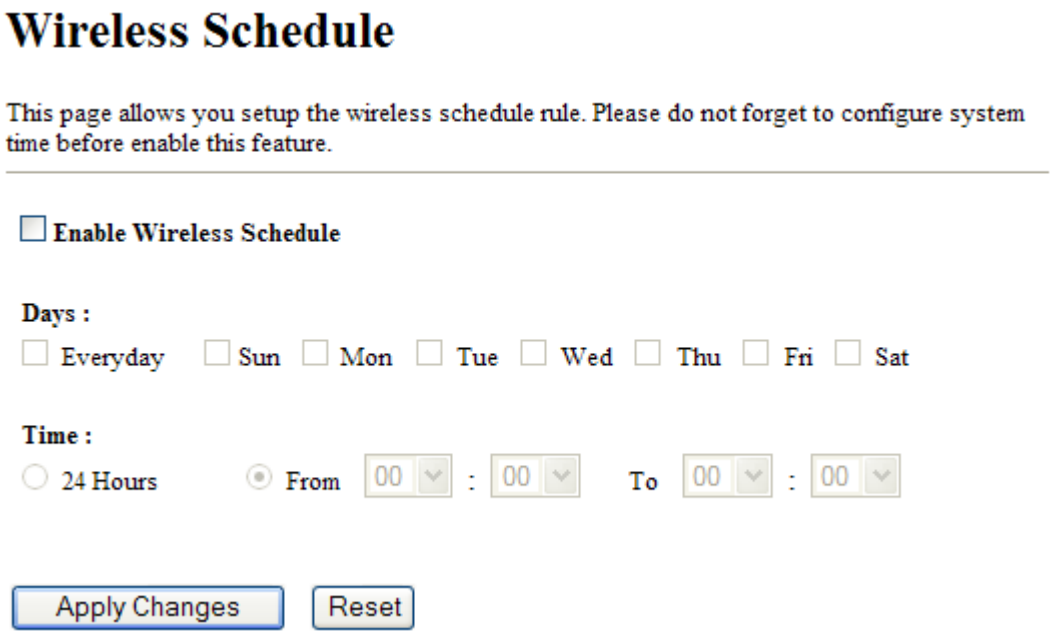
Item	Description
Disable WPS	Click on to disable the Wi-Fi Protected Setup function.
WPS Status	Show WPS status is ***Configured*** or ***UnConfigured***.
Self-PIN Number	Fill in the PIN Number of AP to register the wireless distribution system access capability.
PIN Configuration	The ***Start PIN*** button provides tool to scan the wireless network. If any Access Point or IBSS is found, you could connect it automatically when client join WPS mode.
Push Button Configuration	The ***Start PBC*** button provides tool to scan the wireless network. If any Access Point or IBSS is found, you could

RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

	connect it automatically when client join PBC mode.
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Current Key Info	**Authentication**：It shows the Authentication is opened or closed. **Encryption**：It shows the Encryption mode. **Key**：It shows the Encryption key.

3.3.12 Schedule

This page is to configure the wireless activation timestamp by users.


Wireless Schedule
This page allows you setup the wireless schedule rule. Please do not forget to configure system time before enable this feature.
Enable Wireless Schedule
Days :
Everyday Sun Mon Tue Wed Thu Fri Sat
Time :
24 Hours From 00 : 00 To 00 : 00
Apply Changes
Reset

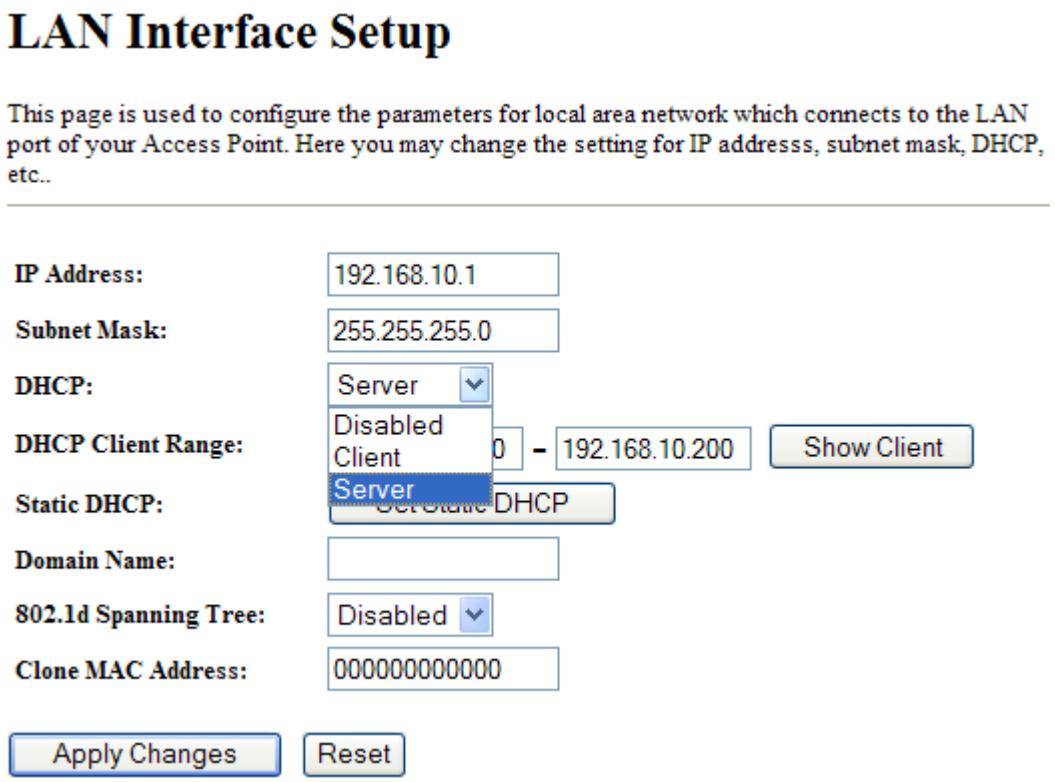
Item	Description
Enable Wireless Schedule	Click on to enable the wireless schedule function.
Days	Click the one or more of days to set the rules.
Time	Click 24 hrs or set the starting time and ending time.
Apply Changes	Click the ***Apply Changes*** button to complete the new

RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

	configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

3.3.13 LAN Interface Setup

This page is used to configure the parameters for local area network that connects to the LAN ports of your WLAN Broadband Router. Here you may change the setting for IP address, subnet mask, DHCP, etc.

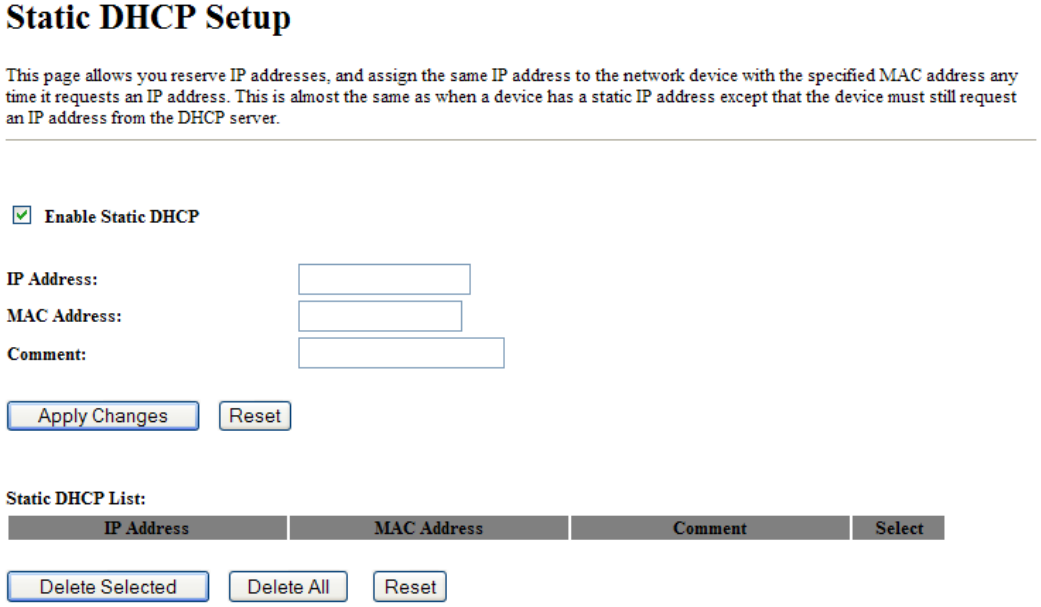


Item	Description
IP Address	Fill in the IP address of LAN interfaces of this WLAN Access Point.
Subnet Mask	Fill in the subnet mask of LAN interfaces of this WLAN Access Point.
DHCP	Click to select ***Disabled***, ***Client*** or ***Server*** in different operation mode of wireless Access Point.
DHCP Client Range	Fill in the start IP address and end IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range.

RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

Show Client	Click to open the ***Active DHCP Client Table*** window that shows the active clients with their assigned IP address, MAC address and time expired information. **[Server mode only]**
Static DHCP	Select enable or disable the Static DHCP function from pull-down menu. **[Server mode only]**
Set Static DHCP	Manual setup Static DHCP IP address for specific MAC address. **[Server mode only]**
Domain Name	Assign Domain Name and dispatch to DHCP clients. It is optional field.
802.1d Spanning Tree	Select enable or disable the IEEE 802.1d Spanning Tree function from pull-down menu.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

I Static DHCP Setup


Static DHCP Setup
This page allows you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the DHCP server.
Enable Static DHCP
IP Address:
MAC Address:
Comment:
Apply Changes
Reset
Static DHCP List:
IP Address
MAC Address
Comment
Select
Delete Selected
Delete All
Reset

Item	Description
Enable Static DHCP	Click on to Enable the Static DHCP Setup function.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

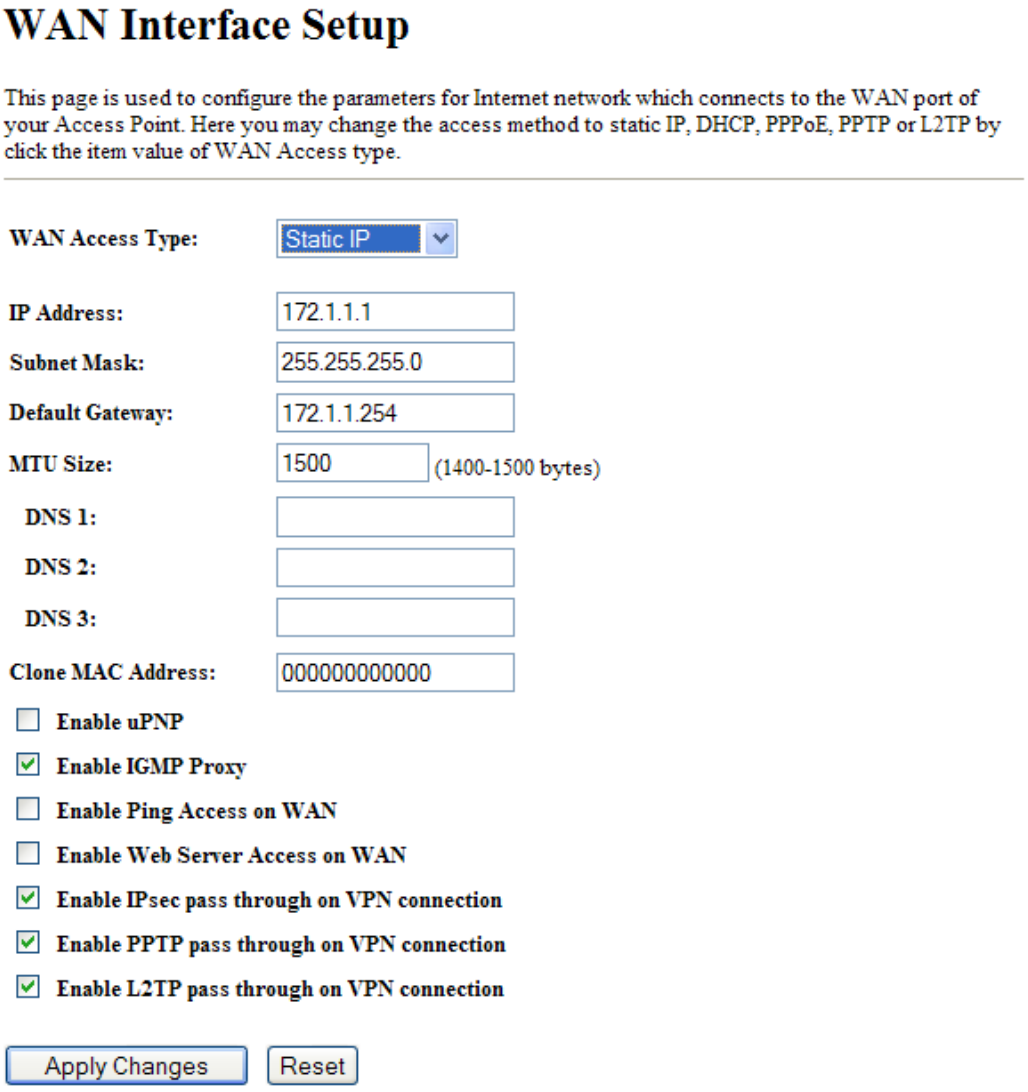
IP Address	If you select the Set Static DHCP on LAN interface, fill in the IP address for it.
MAC Address	If you select the Set Static DHCP on LAN interface, fill in the MAC address for it.
Comment	Fill in the comment tag for the registered Static DHCP.
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Static DHCP List	It shows IP Address、MAC Address from the Static DHCP.
Delete Selected	Click to delete the selected clients that will be removed from the Static DHCP list.
Delete All	Click to delete all the registered clients from the Static DHCP list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

3.3.14 WAN Interface Setup

This page is used to configure the parameters for wide area network that connects to the WAN port of your WLAN Broadband Router. Here you may change the access method to ***Static IP***, ***DHCP***, ***PPPoE, PPTP or L2TP*** by click the item value of **WAN Access Type**. RA-M100Plus also supports **3.5G WAN connection**.

I Static IP


WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.
WAN Access Type:
Static IP
IP Address:
172.1.1.1
Subnet Mask:
255.255.255.0
Default Gateway:
172.1.1.254
MTU Size:
1500
(1400-1500 bytes)
DNS 1:
DNS 2:
DNS 3:
Clone MAC Address:
000000000000
Enable uPNP
Enable IGMP Proxy
Enable Ping Access on WAN
Enable Web Server Access on WAN
Enable IPsec pass through on VPN connection
Enable PPTP pass through on VPN connection
Enable L2TP pass through on VPN connection
Apply Changes
Reset

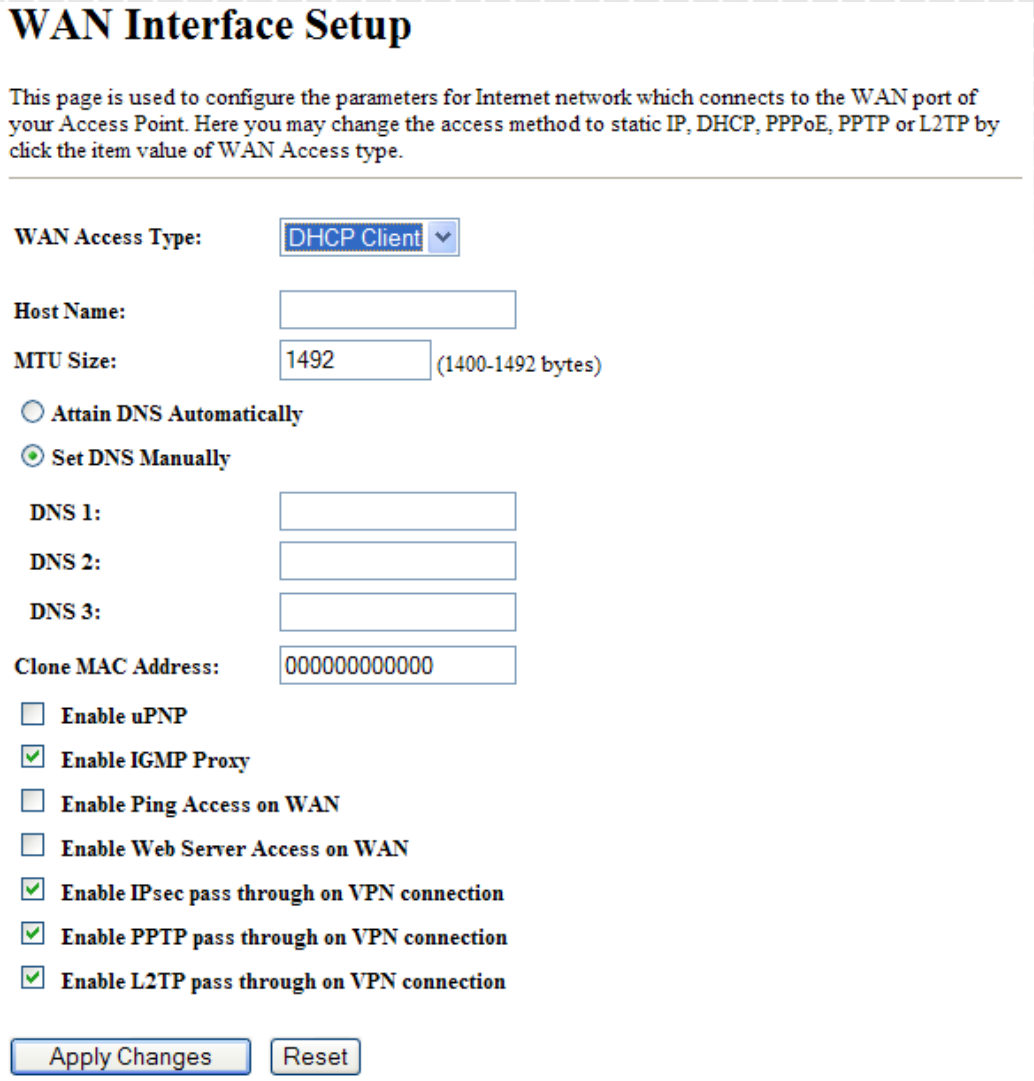
Item	Description
Static IP	Click to select Static IP support on WAN interface. There are IP address, subnet mask and default gateway settings need to be done.
IP Address	If you select the Static IP support on WAN interface, fill in

 Copyright © RayTalk Industries. Tutti i diritti riservati.

	the IP address for it.
Subnet Mask	If you select the Static IP support on WAN interface, fill in the subnet mask for it.
Default Gateway	If you select the Static IP support on WAN interface, fill in the default gateway for WAN interface out going data packets.
MTU Size	Fill in the mtu size of MTU Size. The default value is 1500
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
Enable uPNP	Click the checkbox to enable uPNP function. Refer to 4.22 What is Universal Plug and Play (uPNP)?
Enable IGMP Proxy	Click the checkbox to enable IGMP Proxy.
Enable Ping Access on WAN	Click the checkbox to enable WAN ICMP response.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Enable IPsec pass through on VPN connection	Click the checkbox to enable IPSec packet pass through
Enable PPTP pass through on VPN connection	Click the checkbox to enable PPTP packet pass through
Enable L2TP pass through on VPN connection	Click the checkbox to enable L2TP packet pass through
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

II DHCP Client


WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.
WAN Access Type:
DHCP Client
Host Name:
MTU Size:
1492
(1400-1492 bytes)
Attain DNS Automatically
Set DNS Manually
DNS 1:
DNS 2:
DNS 3:
Clone MAC Address:
000000000000
Enable uPNP
Enable IGMP Proxy
Enable Ping Access on WAN
Enable Web Server Access on WAN
Enable IPsec pass through on VPN connection
Enable PPTP pass through on VPN connection
Enable L2TP pass through on VPN connection
Apply Changes
Reset

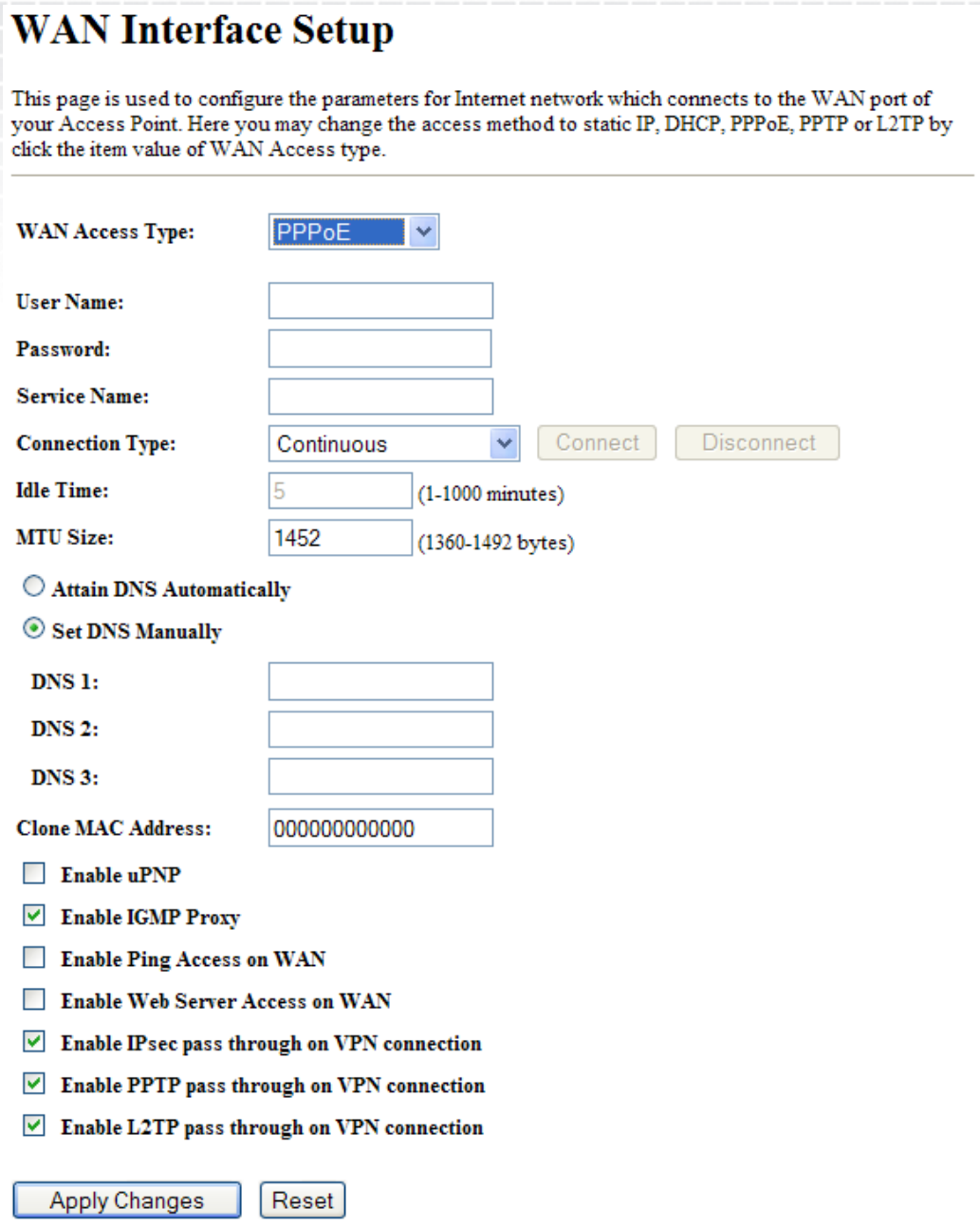
Item	Description
DHCP Client	Click to select DHCP support on WAN interface for IP address assigned automatically from a DHCP server.
Host Name	Fill in the host name of Host Name. The default value is empty
MTU Size	Fill in the mtu size of MTU Size. The default value is 1492
Attain DNS Automatically	Click to select getting DNS address for ***DHCP*** support. Please select ***Set DNS Manually*** if the ***DHCP*** support is selected.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

Set DNS Manually	Click to select getting DNS address for ***DHCP*** support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
Enable uPNP	Click the checkbox to enable uPNP function. Refer to 4.22 What is Universal Plug and Play (uPNP)?
Enable IGMP Proxy	Click the checkbox to enable IGMP Proxy.
Enable Ping Access on WAN	Click the checkbox to enable WAN ICMP response.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

III PPPoE



Item	Description
PPPoE	Click to select PPPoE support on WAN interface. There are user name, password, connection type and idle time settings need to be done.
User Name	If you select the PPPoE support on WAN interface, fill in the user name and password to login the PPPoE server.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

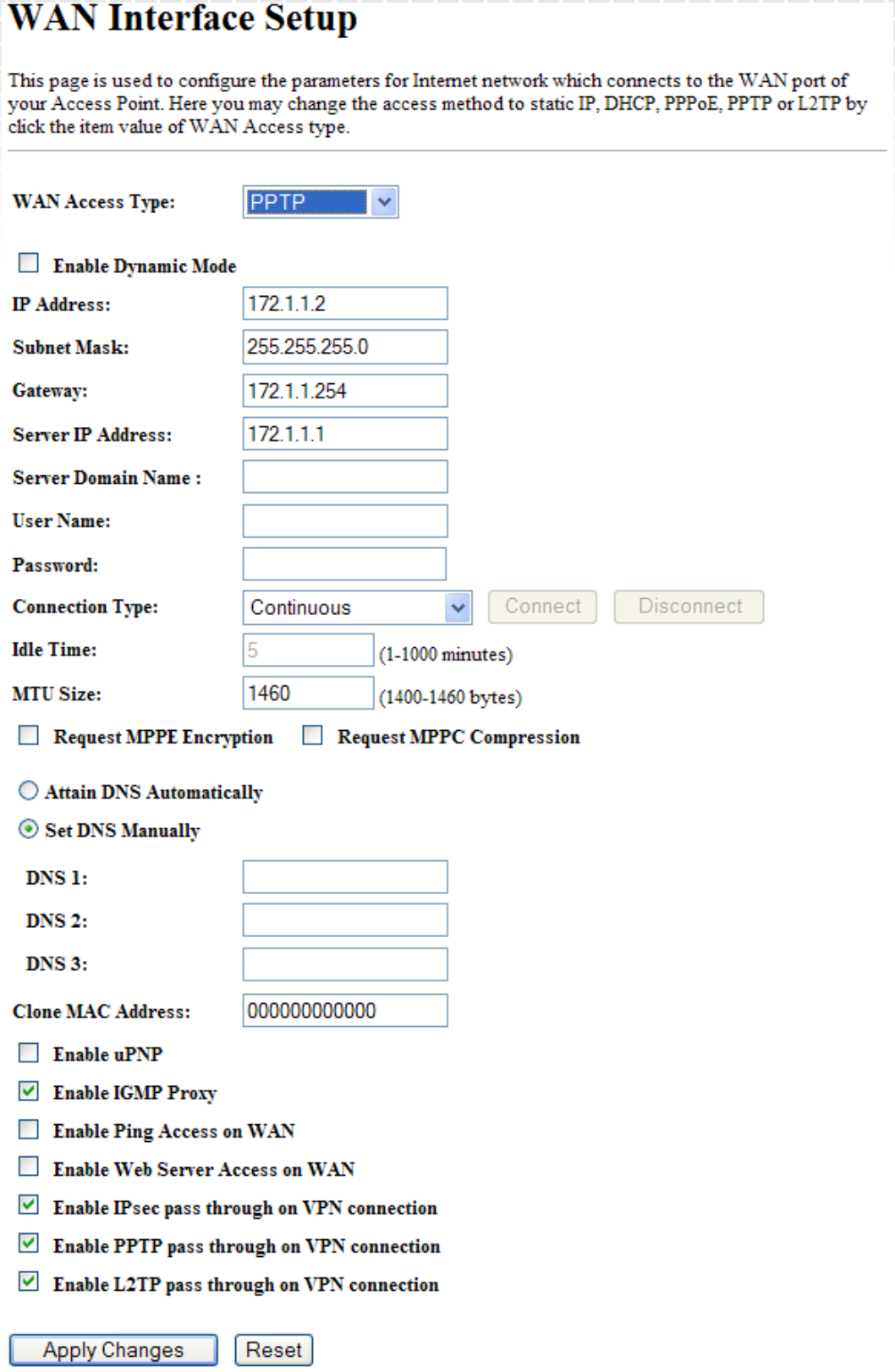
Password	If you select the PPPoE support on WAN interface, fill in the user name and password to login the PPPoE server.
Service Name	Fill in the service name of Service Name. The default value is empty.
Connection Type	Select the connection type from pull-down menu. There are ***Continuous***, ***Connect on Demand*** and ***Manual*** three types to select. ***Continuous*** connection type means to setup the connection through PPPoE protocol whenever this WLAN Broadband Router is powered on. ***Connect on Demand*** connection type means to setup the connection through PPPoE protocol whenever you send the data packets out through the WAN interface; there are a watchdog implemented to close the PPPoE connection while there are no data sent out longer than the idle time set. ***Manual*** connection type means to setup the connection through the PPPoE protocol by clicking the ***Connect*** button manually, and clicking the ***Disconnect*** button manually.
Idle Time	If you select the ***PPPoE*** and ***Connect on Demand*** connection type, fill in the idle time for auto-disconnect function. Value can be between 1 and 1000 minutes.
MTU Size	Fill in the mtu size of MTU Size. The default value is 1452. Refer to 4.23 What is Maximum Transmission Unit (MTU) Size?
Attain DNS Automatically	Click to select getting DNS address for ***PPPoE*** support. Please select ***Set DNS Manually*** if the ***PPPoE*** support is selected.
Set DNS Manually	Click to select getting DNS address for ***Static IP*** support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
Enable uPNP	Click the checkbox to enable uPNP function. Refer to 4.22 What is Universal Plug and Play (uPNP)?
Enable IGMP Proxy	Click the checkbox to enable IGMP Proxy.
Enable Ping Access on WAN	Click the checkbox to enable WAN ICMP response.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

IV PPTP



 Copyright © RayTalk Industries. Tutti i diritti riservati.

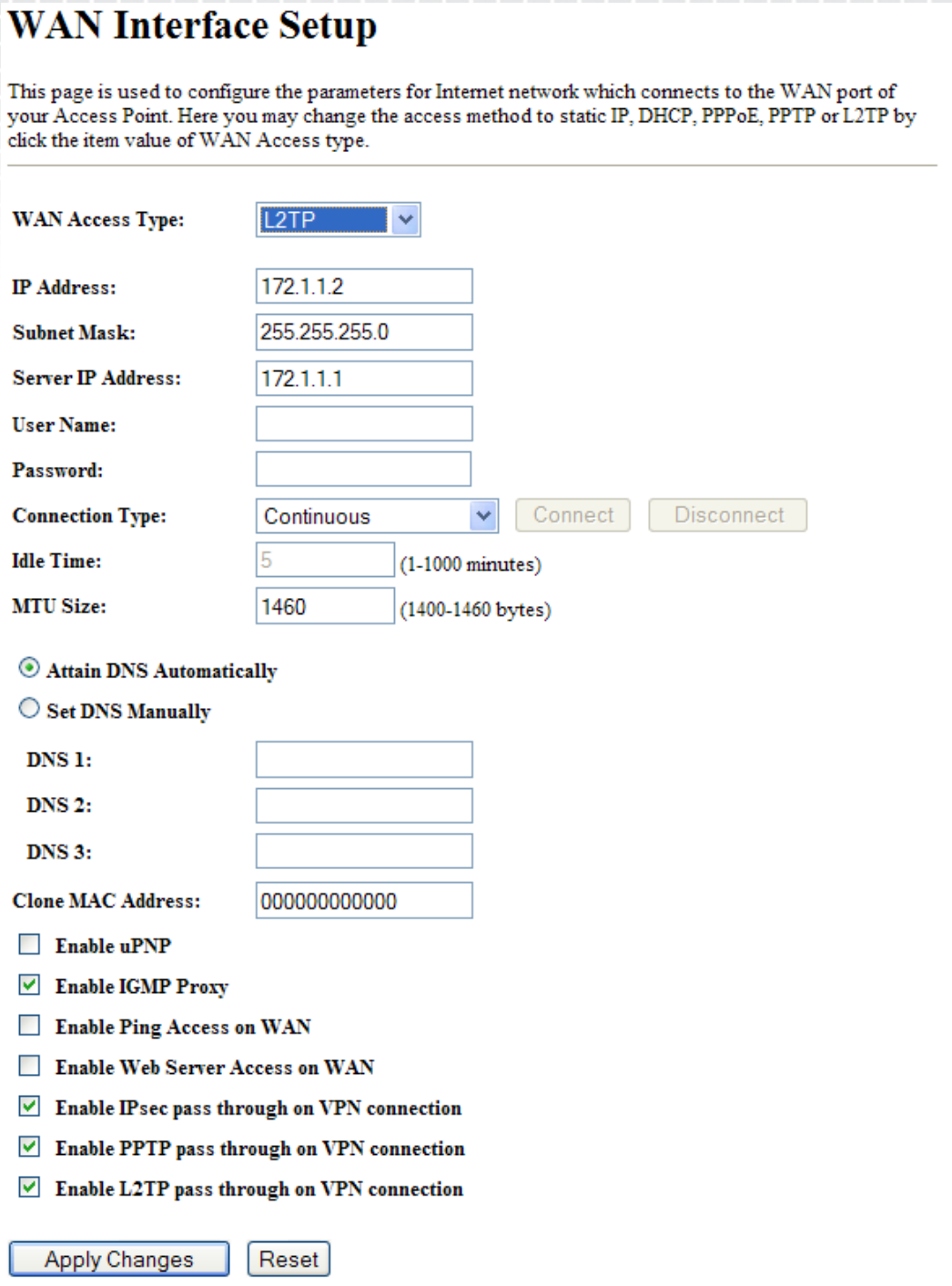
Item	Description
PPTP	Allow user to make a tunnel with remote site directly to secure the data transmission among the connection. User can use embedded PPTP client supported by this router to make a VPN connection.
Enable Dynamic Mode	Click the checkbox to enable Dynamic PPTP function.
IP Address	If you select the PPTP support on WAN interface, fill in the IP address for it.
Subnet Mask	If you select the PPTP support on WAN interface, fill in the subnet mask for it.
Server IP Address	Enter the IP address of the PPTP Server.
Server Domain Name	Input domain name to resolve DHCP server.
User Name	If you select the PPTP support on WAN interface, fill in the user name and password to login the PPTP server.
Password	If you select the PPTP support on WAN interface, fill in the user name and password to login the PPTP server.
Connection Type	Select the connection type from pull-down menu. There are ***Continuous***, ***Connect on Demand*** and ***Manual*** three types to select. ***Continuous*** connection type means to setup the connection through PPTP protocol whenever this WLAN Broadband Router is powered on. ***Connect on Demand*** connection type means to setup the connection through PPTP protocol whenever you send the data packets out through the WAN interface; there are a watchdog implemented to close the PPTP connection while there are no data sent out longer than the idle time set. ***Manual*** connection type means to setup the connection through the PPTP protocol by clicking the ***Connect*** button manually, and clicking the ***Disconnect*** button manually.
Idle Time	If you select the ***PPTP*** and ***Connect on Demand***

 Copyright © RayTalk Industries. Tutti i diritti riservati.

	connection type, fill in the idle time for auto-disconnect function. Value can be between 1 and 1000 minutes.
MTU Size	Fill in the mtu size of MTU Size. The default value is 1460. Refer to 4.23 What is Maximum Transmission Unit (MTU) Size?
Request MPPE Encryption	Click the checkbox to enable request MPPE encryption.
Request MPPC Compression	Click the checkbox to enable request MPPC compression.
Attain DNS Automatically	Click to select getting DNS address for ***PPTP*** support. Please select ***Set DNS Manually*** if the ***PPTP*** support is selected.
Set DNS Manually	Click to select getting DNS address for ***PPTP*** support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
Enable uPNP	Click the checkbox to enable uPNP function. Refer to 4.22 What is Universal Plug and Play (uPNP)?
Enable IGMP Proxy	Click the checkbox to enable IGMP Proxy.
Enable Ping Access on WAN	Click the checkbox to enable WAN ICMP response.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

V L2TP



Item	Description
L2TP	Allow user to make a tunnel with remote site directly to secure the data transmission among the connection. User can use embedded L2TP client supported by this router to make a VPN connection.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

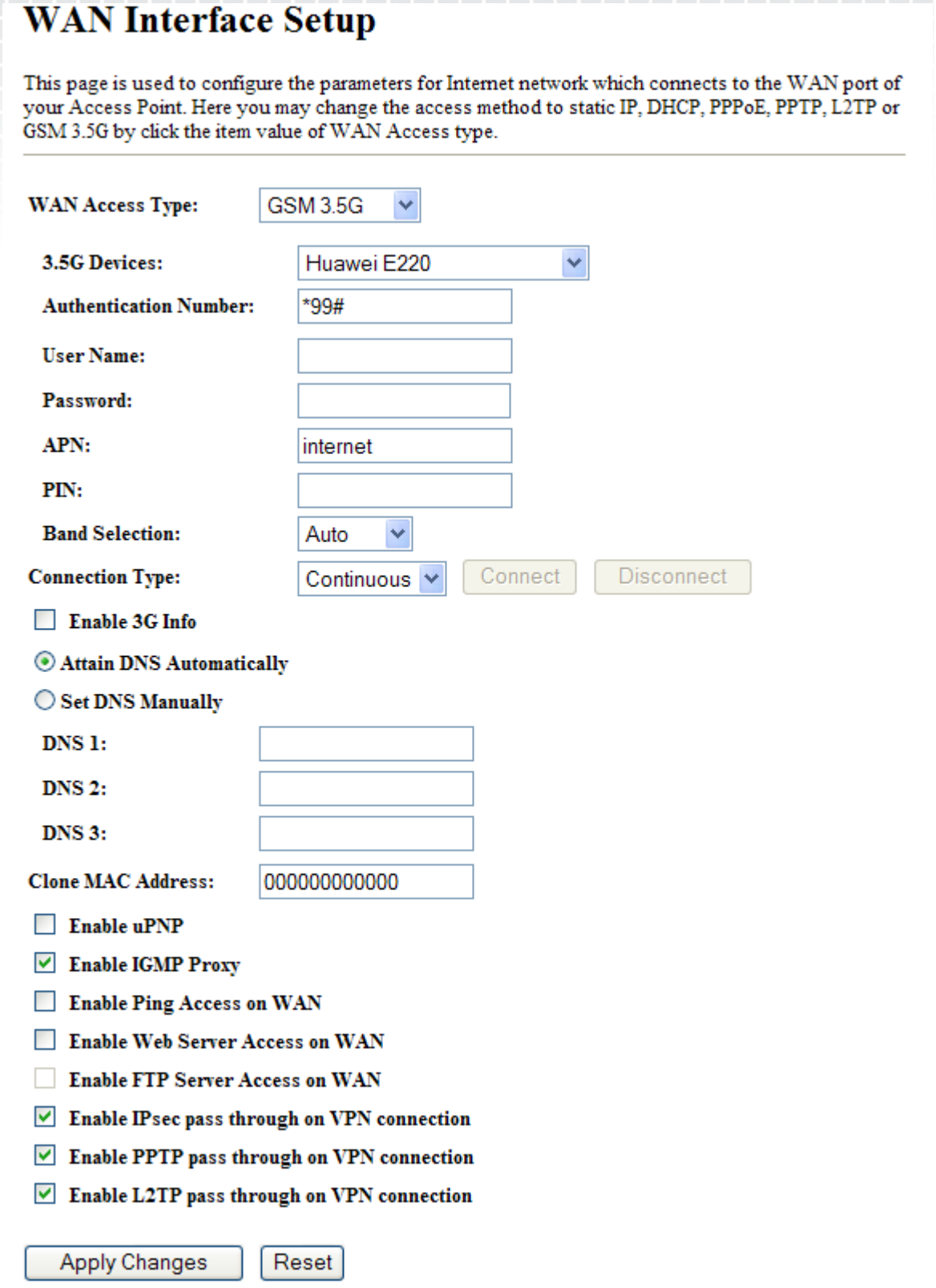
IP Address	If you select the L2TP support on WAN interface, fill in the IP address for it.
Subnet Mask	If you select the L2TP support on WAN interface, fill in the subnet mask for it.
Gateway	If you select the Static L2TP support on WAN interface, fill in the gateway for WAN interface out going data packets.
Server IP Address	Enter the IP address of the L2TP Server.
User Name	If you select the L2TP support on WAN interface, fill in the user name and password to login the L2TP server.
Password	f you select the L2TP support on WAN interface, fill in the user name and password to login the L2TP server.
Connection Type	Select the connection type from pull-down menu. There are ***Continuous***, ***Connect on Demand*** and ***Manual*** three types to select. ***Continuous*** connection type means to setup the connection through L2TP protocol whenever this WLAN Broadband Router is powered on. ***Connect on Demand*** connection type means to setup the connection through L2TP protocol whenever you send the data packets out through the WAN interface; there are a watchdog implemented to close the L2TP connection while there are no data sent out longer than the idle time set. ***Manual*** connection type means to setup the connection through the L2TP protocol by clicking the ***Connect*** button manually, and clicking the ***Disconnect*** button manually.
Idle Time	If you select the ***L2TP*** and ***Connect on Demand*** connection type, fill in the idle time for auto-disconnect function. Value can be between 1 and 1000 minutes.
MTU Size	Fill in the mtu size of MTU Size. The default value is 1460. Refer to 4.23 What is Maximum Transmission Unit (MTU) Size?

 Copyright © RayTalk Industries. Tutti i diritti riservati.

Attain DNS Automatically	Click to select getting DNS address for ***L2TP*** support. Please select ***Set DNS Manually*** if the ***L2TP*** support is selected.
Set DNS Manually	Click to select getting DNS address for ***L2TP*** support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
Enable uPNP	Click the checkbox to enable uPNP function. Refer to 4.22 What is Universal Plug and Play (uPNP)?
Enable IGMP Proxy	Click the checkbox to enable IGMP Proxy.
Enable Ping Access on WAN	Click the checkbox to enable WAN ICMP response.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

VI GSM 3.5G (RA-M100Plus only)



 Copyright © RayTalk Industries. Tutti i diritti riservati.

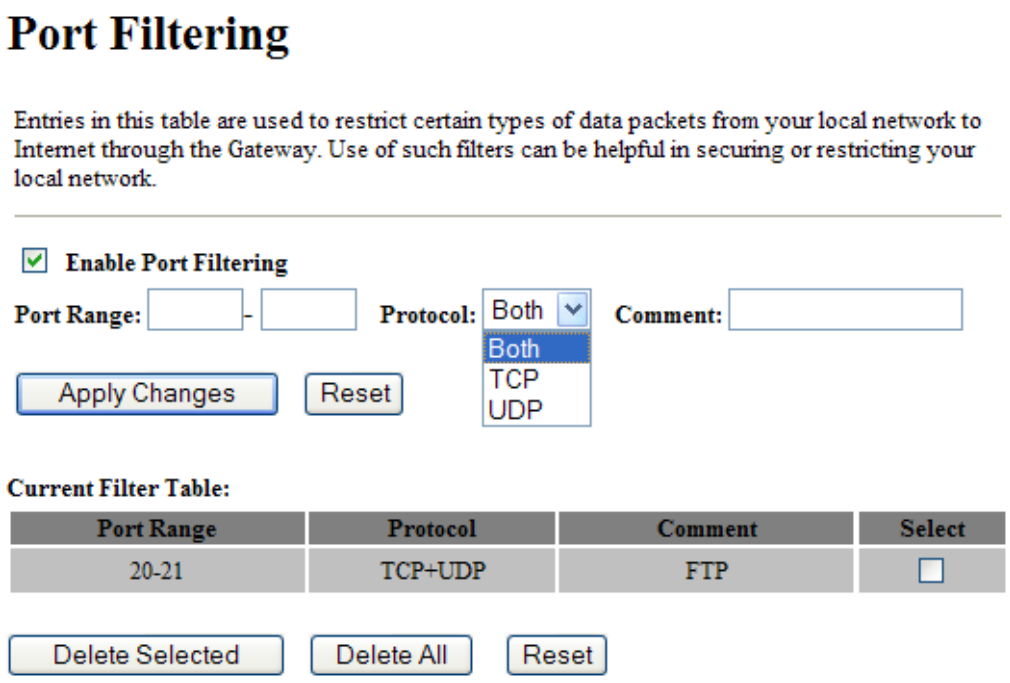
Item	Description
GSM 3.5	Click to select 3.5G support for WAN Interface. This feature is available connecting a 3G USB dongle to the USB port.
3.5G Devices	Choose the USB Dongle model from a list of compatible devices. 4.36 Which 3.5G devices are compatible with RA-M100Plus?
Authentication Number	Enter the Authentication Number from Mobile Operator. Default is *99#.
User Name	Enter the User Name from Mobile Operator. Usually not needed.
Password	Enter the Password from Mobile Operator. Usually not needed.
APN	Enter the Mobile Operator APN. Default is internet.
PIN	Enter the SIM card PIN number if PIN I enable on 3G SIM.
Band Selection	Choose the Mobile Band: Auto, 3G only or 2G only. Default is Auto.
Connection Type	Choose the connection type: Continuous or Manual. Default is Continuous.
Enable 3G info	Enable/Disable 3G information on STATUS page.
Attain DNS Automatically	Click to select getting DNS address for ***L2TP*** support. Please select ***Set DNS Manually*** if the ***GSM 3.5*** support is selected.
Set DNS Manually	Click to select getting DNS address for ***Static IP*** support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
Enable uPNP	Click the checkbox to enable uPNP function. Refer to 4.22 What is Universal Plug and Play

 Copyright © RayTalk Industries. Tutti i diritti riservati.

	(uPNP)?
Enable IGMP Proxy	Click the checkbox to enable IGMP Proxy.
Enable Ping Access on WAN	Click the checkbox to enable WAN ICMP response.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

3.3.15 Firewall - Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.



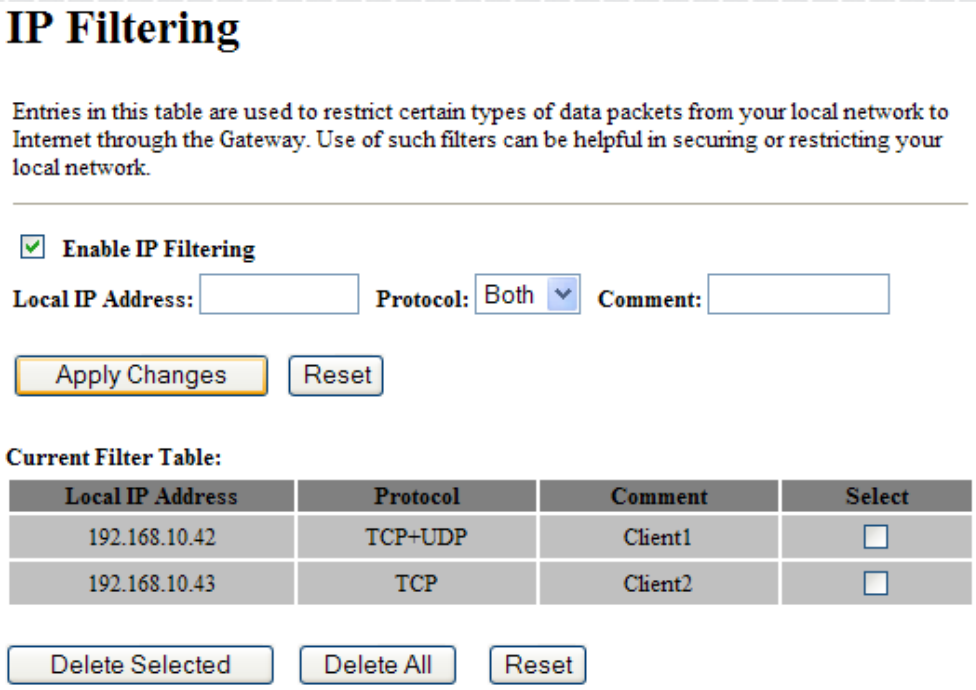
 Copyright © RayTalk Industries. Tutti i diritti riservati.

Item	Description
Enable Port Filtering	Click to enable the port filtering security function.
Port Range Protocol Comments	To restrict data transmission from the local network on certain ports, fill in the range of start-port and end-port, and the protocol, also put your comments on it. The ***Protocol*** can be TCP, UDP or Both. ***Comments*** let you know about whys to restrict data from the ports.
Apply Changes	Click the ***Apply Changes*** button to register the ports to port filtering list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected port range that will be removed from the port-filtering list.
Delete All	Click to delete all the registered entries from the port-filtering list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

3.3.16 Firewall - IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

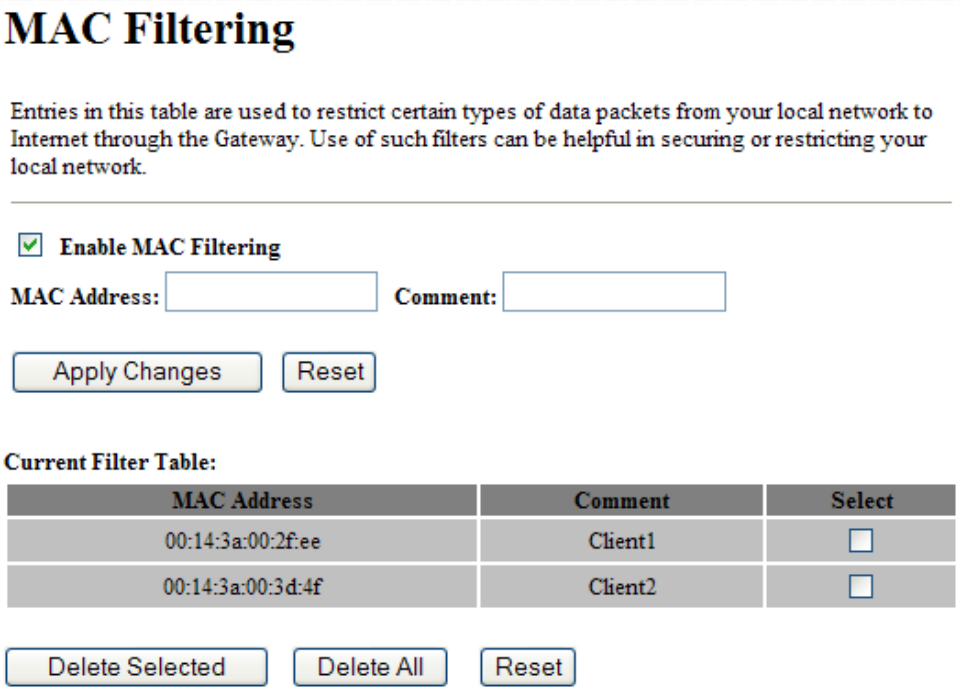


Item	Description
Enable IP Filtering	Click to enable the IP filtering security function.
Local IP Address Protocol Comments	To restrict data transmission from local network on certain IP addresses, fill in the IP address and the protocol, also put your comments on it. The ***Protocol*** can be TCP, UDP or Both. ***Comments*** let you know about whys to restrict data from the IP address.
Apply Changes	Click the ***Apply Changes*** button to register the IP address to IP filtering list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected IP address that will be removed from the IP-filtering list.
Delete All	Click to delete all the registered entries from the IP-filtering list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

3.3.17 Firewall - MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.



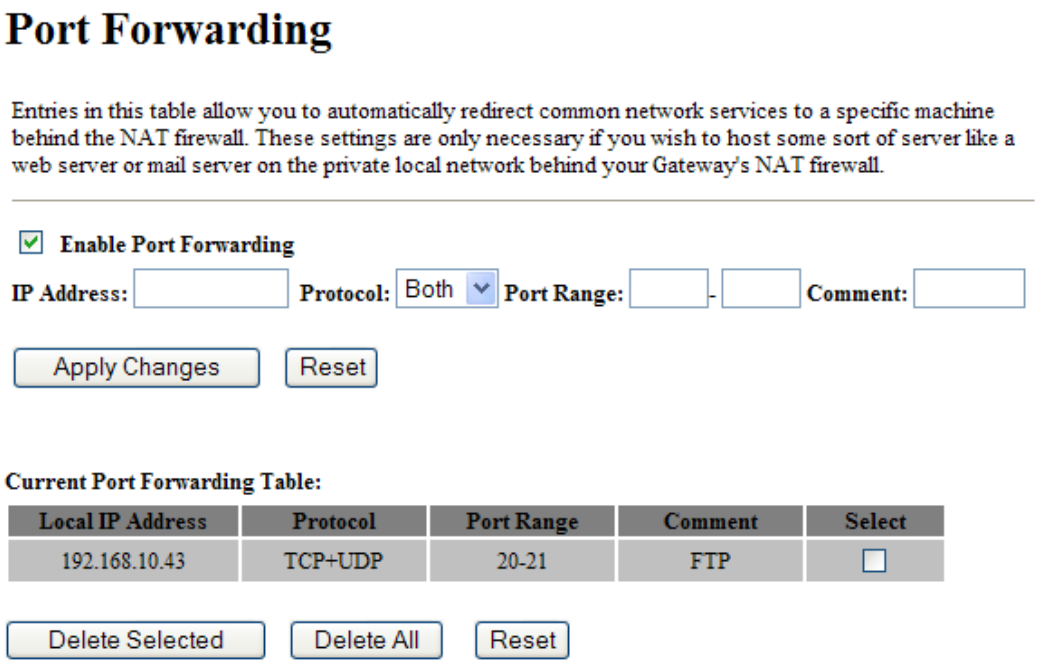
Item	Description
Enable MAC Filtering	Click to enable the MAC filtering security function.
MAC Address Comments	To restrict data transmission from local network on certain MAC addresses, fill in the MAC address and your comments on it. ***Comments*** let you know about whys to restrict data from the MAC address.
Apply Changes	Click the ***Apply Changes*** button to register the MAC address to MAC filtering list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected MAC address that will be removed from the MAC-filtering list.
Delete All	Click to delete all the registered entries from the MAC-filtering list.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

3.3.18 Firewall - Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.


Port Forwarding
Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.
Enable Port Forwarding
IP Address:
Protocol: Both
Port Range:
Comment:
Apply Changes
Reset
Current Port Forwarding Table:
Local IP Address
Protocol
Port Range
Comment
Select
192.168.10.43
TCP+UDP
20-21
FTP
Delete Selected
Delete All
Reset

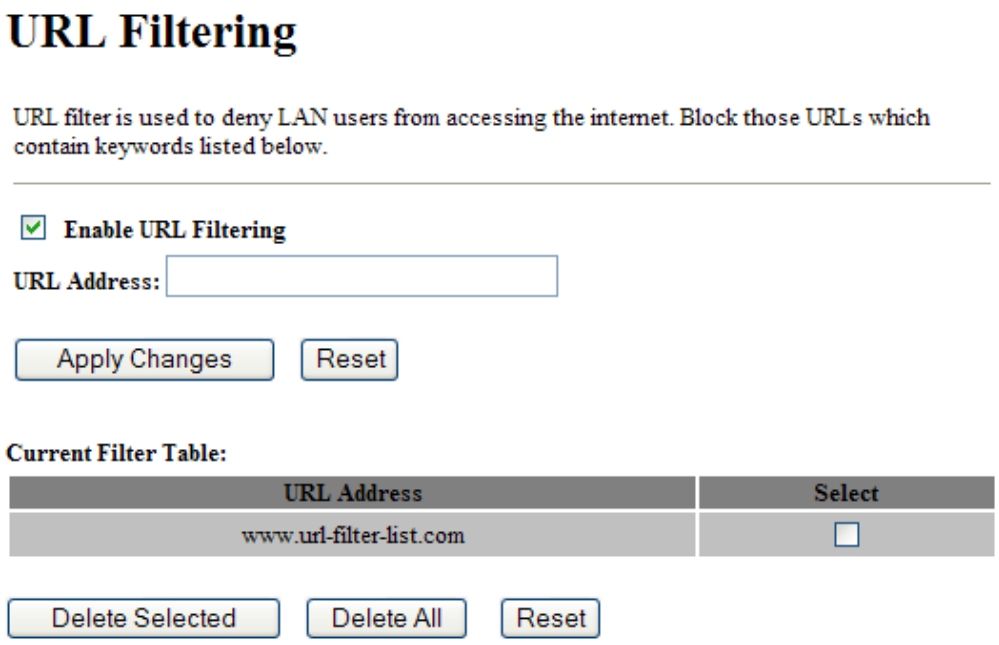
Item	Description
Enable Port Forwarding	Click to enable the Port Forwarding security function.
IP Address Protocol Port Range Comment	To forward data packets coming from WAN to a specific IP address that hosted in local network behind the NAT firewall, fill in the IP address, protocol, port range and your comments. The ***Protocol*** can be TCP, UDP or Both. The ***Port Range*** for data transmission.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

	Comments let you know about whys to allow data packets forward to the IP address and port number.
Apply Changes	Click the ***Apply Changes*** button to register the IP address and port number to Port forwarding list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected IP address and port number that will be removed from the port-forwarding list.
Delete All	Click to delete all the registered entries from the port-forwarding list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

3.3.19 Firewall – URL Filtering

URL Filtering is used to restrict users to access specific websites in internet.



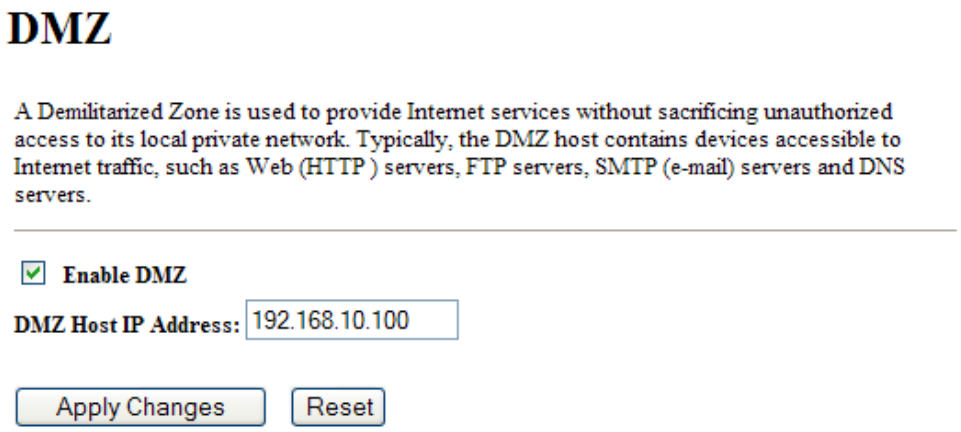
Item	Description
Enable URL Filtering	Click to enable the URL Filtering function.
URL Address	Add one URL address.
Apply Changes	Click the ***Apply Changes*** button to save settings.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

Delete Selected	Click to delete the selected URL address that will be removed from the URL Filtering list.
Delete All	Click to delete all the registered entries from the URL Filtering list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

3.3.20 Firewall - DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

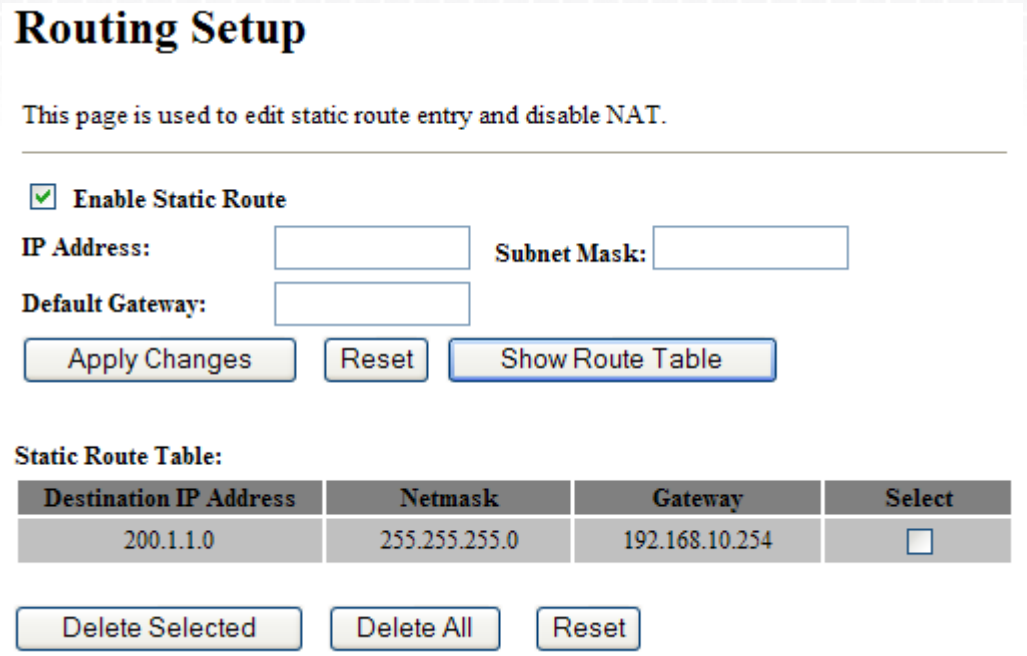

DMZ
A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.
Enable DMZ
DMZ Host IP Address:
192.168.10.100
Apply Changes
Reset

Item	Description
Enable DMZ	Click to enable the DMZ function.
DMZ Host IP Address	To support DMZ in your firewall design, fill in the IP address of DMZ host that can be access from the WAN interface.
Apply Changes	Click the ***Apply Changes*** button to register the IP address of DMZ host.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

3.3.21 Routing Setup

This page is used to edit static route entry and disable NAT. This feature is available only on RA-M100Plus and firmware starting from u2.3.0.3.R00.



Item	Description
Enable Static Route	Click to enable the Static Route.
IP Address:	Insert the destination IP Address or Network.
Subnet Mask	Insert the destination Subnet Mask.
Default Gateway	Insert the Default Gateway within the source Network.
Apply Changes	Click the ***Apply Changes*** button to add settings to the list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Show Route Table	This table shows all the routing entry.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

Routing Table

This table shows the all routing entry .

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
239.255.255.250	0.0.0.0	255.255.255.255	UH	0	0	0	br0
200.1.1.0	192.168.10.254	255.255.255.0	UG	0	0	0	br0
192.168.10.0	0.0.0.0	255.255.255.0	U	0	0	0	br0

Refresh Close

3.3.22 QoS

This page sets bandwidth control by IP or Mac address.

QoS

Entries in this table improve your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.

Enable QoS

Automatic Uplink Speed

Manual Uplink Speed (Kbps): 512

Automatic Downlink Speed

Manual Downlink Speed (Kbps): 0

QoS Rule Setting:

Address Type: IP MAC

Local IP Address: -

MAC Address:

Mode: Guaranteed minimum bandwidth

Uplink Bandwidth (Kbps):

Downlink Bandwidth (Kbps):

Comment:

Apply Changes Reset

Current QoS Rules Table:

Local IP Address	MAC Address	Mode	Uplink Bandwidth	Downlink Bandwidth	Comment	Select

Delete Selected Delete All Reset

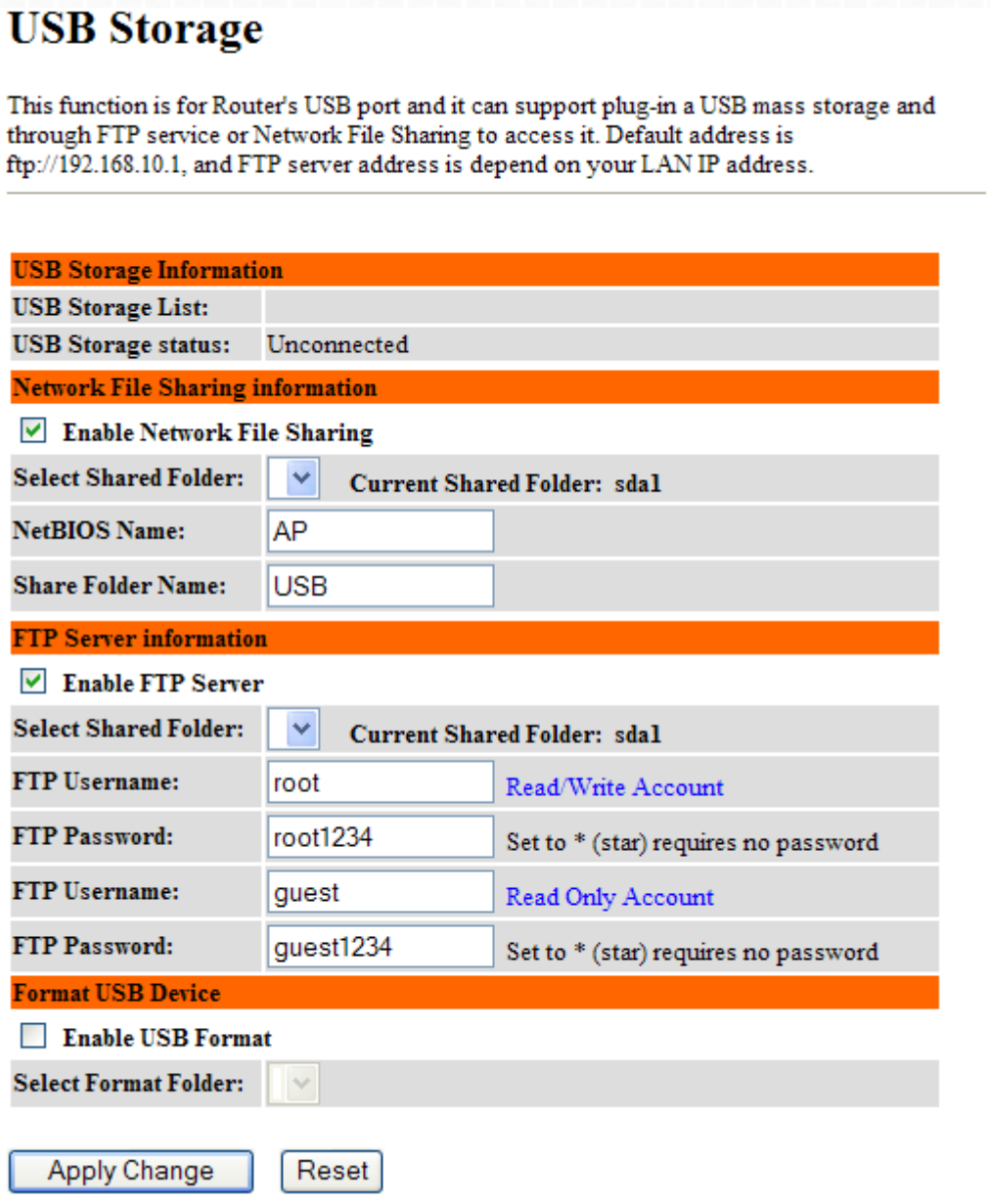
 Copyright © RayTalk Industries. Tutti i diritti riservati.

Item	Description
Enable QoS	Click to enable the QoS function.
Automatic Uplink Speed	Click checkbox to enable Uplink speed by system.
Manual Uplink Speed (Kbps)	Input number to set Uplink speed.
Automatic Downlink Speed	Click checkbox to enable Downlink speed by system.
Manual Downlink Speed (Kbps)	Input number to set Downlink speed.
Access Type	Click the set type either IP or Mac address.
Local IP address	Input the range IP address of LAN.
MAC address	Input MAC address.
Mode	There are 2 options to control the bandwidth. One is ***Guaranteed minimum bandwidth***. The other is ***Restricted maximum bandwidth***.
Uplink Bandwidth (Kbps)	Set Uplink bandwidth for range of IP addresses or specific MAC address
Downlink Bandwidth (Kbps)	Set Downlink bandwidth for range of IP addresses or specific MAC address
Comment	***Comments*** let you to remind your settings easily.
Apply Changes	Click the ***Apply Changes*** button to add settings to the list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

3.3.23 USB Storage

This page provides USB Storage management like USB link status, Network File Sharing, FTP Server and USB FAT32 format tool. USB Storage File System support FAT32 and EXT2 to Read / Write, NTFS support Read only. (FAT32 only support 32GB for space and 2G for a file).


USB Storage
This function is for Router's USB port and it can support plug-in a USB mass storage and through FTP service or Network File Sharing to access it. Default address is ftp://192.168.10.1, and FTP server address is depend on your LAN IP address.
USB Storage Information
USB Storage List:
USB Storage status: Unconnected
Network File Sharing information
Enable Network File Sharing
Select Shared Folder: Current Shared Folder: sda1
NetBIOS Name: AP
Share Folder Name: USB
FTP Server information
Enable FTP Server
Select Shared Folder: Current Shared Folder: sda1
FTP Username: root Read/Write Account
FTP Password: root1234 Set to * (star) requires no password
FTP Username: guest Read Only Account
FTP Password: guest1234 Set to * (star) requires no password
Format USB Device
Enable USB Format
Select Format Folder:
Apply Change
Reset

Item	Description
USB Storage Information	
USB Storage List	It lists mounted USB Storage ID.

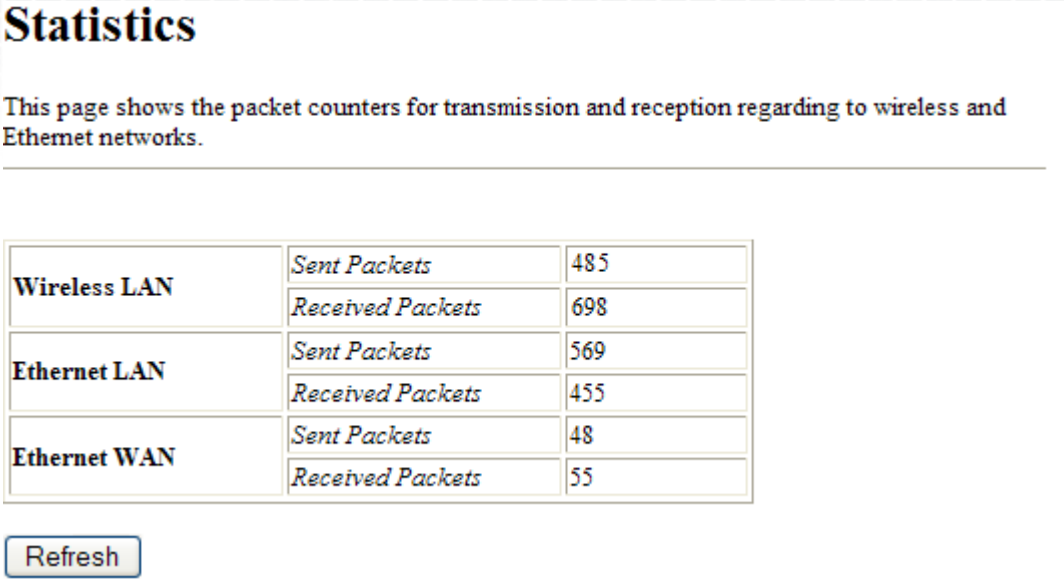
 Copyright © RayTalk Industries. Tutti i diritti riservati.

USB Storage Status	It shows USB Storage link status.
Network File Sharing Information	
Enable Network File Sharing	Click to enable *Network File Sharing.*
Select Share Folder	Click drop down menu to select which USB Storage is going to be shared.
Current Share Folder	It shows the current USB storage share folder.
NetBIOS Name	Input *NetBIOS* name. Maximal 30 characters.
Share Folder Name	Input *Share Folder* name. Maximal 30 characters.
FTP Server Information	
Enable FTP Server	Click to enable *FTP Server*.
Select Share Folder	Click drop down menu to select which USB Storage is going to be set as *FTP Server*.
Current Share Folder	It shows the current FTP USB Server.
FTP Username: (Read/Write Account)	Assign FTP Server Login Name. Default is *root*. Read/Write Account.
FTP Password: (Read/Write Account)	Assign FTP Server Password. Default is *root1234*. Read/Write Account.
FTP Username: (Read Only Account)	Assign FTP Server Login Name. Default is *guest*. Read Only Account.
FTP Password: (Read Only Account)	Assign FTP Server Password. Default is *guest1234*. Read Only Account.
Format USB Device	
Enable USB Format	Click to enable USB Storage format tool.
Select Format Folder	Click on drop down menu to select which USB Storage is going to be formatted to FAT32.
Apply Changes	Click the ***Apply Changes*** button to add settings to the list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

3.3.24 Management - Statistics

This page shows the packet counters for transmission and reception regarding to wireless, Ethernet LAN and Ethernet WAN networks.



Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Wireless LAN	*Sent Packets*	485
	Received Packets	698
Ethernet LAN	*Sent Packets*	569
	Received Packets	455
Ethernet WAN	*Sent Packets*	48
	Received Packets	55

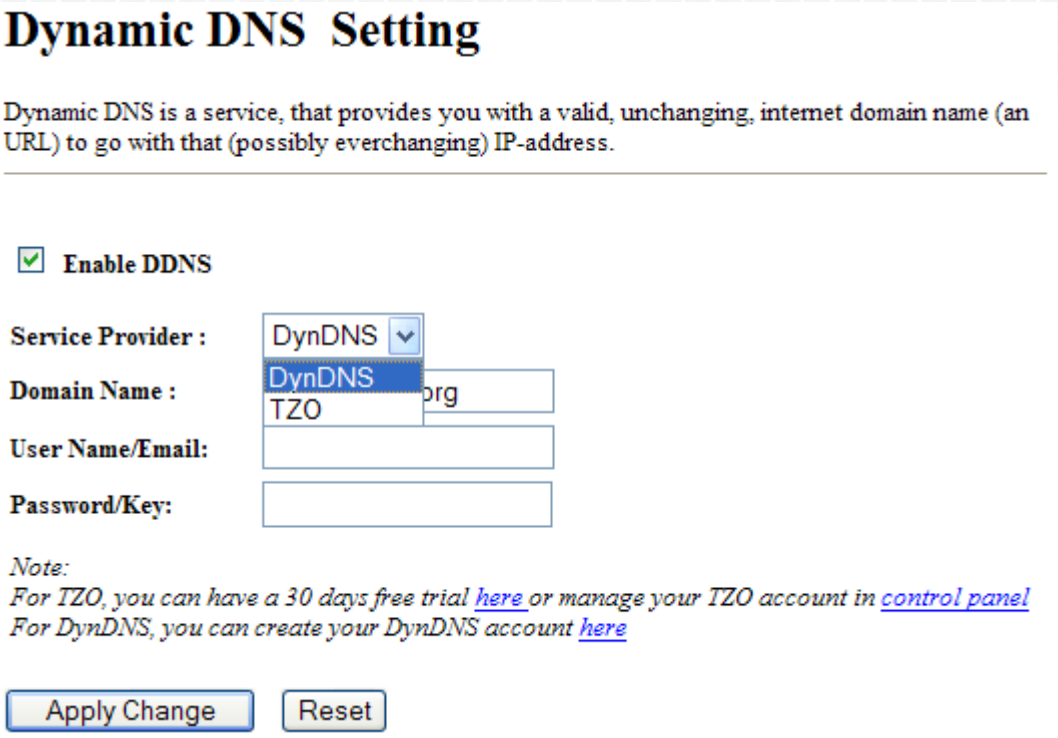
Refresh

Item	Description
Wireless LAN ***Sent Packets***	It shows the statistic count of sent packets on the wireless LAN interface.
Wireless LAN ***Received Packets***	It shows the statistic count of received packets on the wireless LAN interface.
Ethernet LAN ***Sent Packets***	It shows the statistic count of sent packets on the Ethernet LAN interface.
Ethernet LAN ***Received Packets***	It shows the statistic count of received packets on the Ethernet LAN interface.
Ethernet WAN ***Sent Packets***	It shows the statistic count of sent packets on the Ethernet WAN interface.
Ethernet WAN ***Received Packets***	It shows the statistic count of received packets on the Ethernet WAN interface.
Refresh	Click the refresh the statistic counters on the screen.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

3.3.25 Management - DDNS

This page is used to configure Dynamic DNS service to have DNS with dynamic IP address.

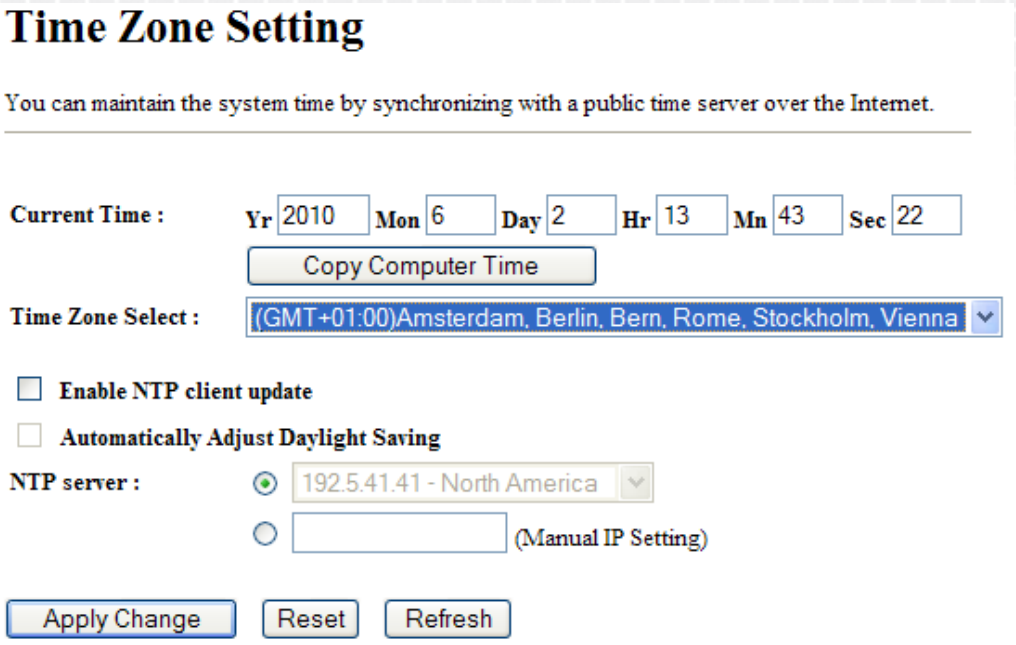

Dynamic DNS Setting
Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.
Enable DDNS
Service Provider :
DynDNS
DynDNS
TZO
Domain Name :
User Name/Email:
Password/Key:
Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here
Apply Change
Reset

Item	Description
Enable DDNS	Click the checkbox to enable ***DDNS*** service. Refer to 4.25 What is DDNS?
Service Provider	Click the drop down menu to pickup the right provider.
Domain Name	To configure the Domain Name.
User Name/Email	Configure User Name, Email.
Password/Key	Configure Password, Key.
Apply Change	Click the ***Apply Changes*** button to save the enable DDNS service.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

3.3.26 Management - Time Zone Setting

This page is used to configure NTP client to get current time.

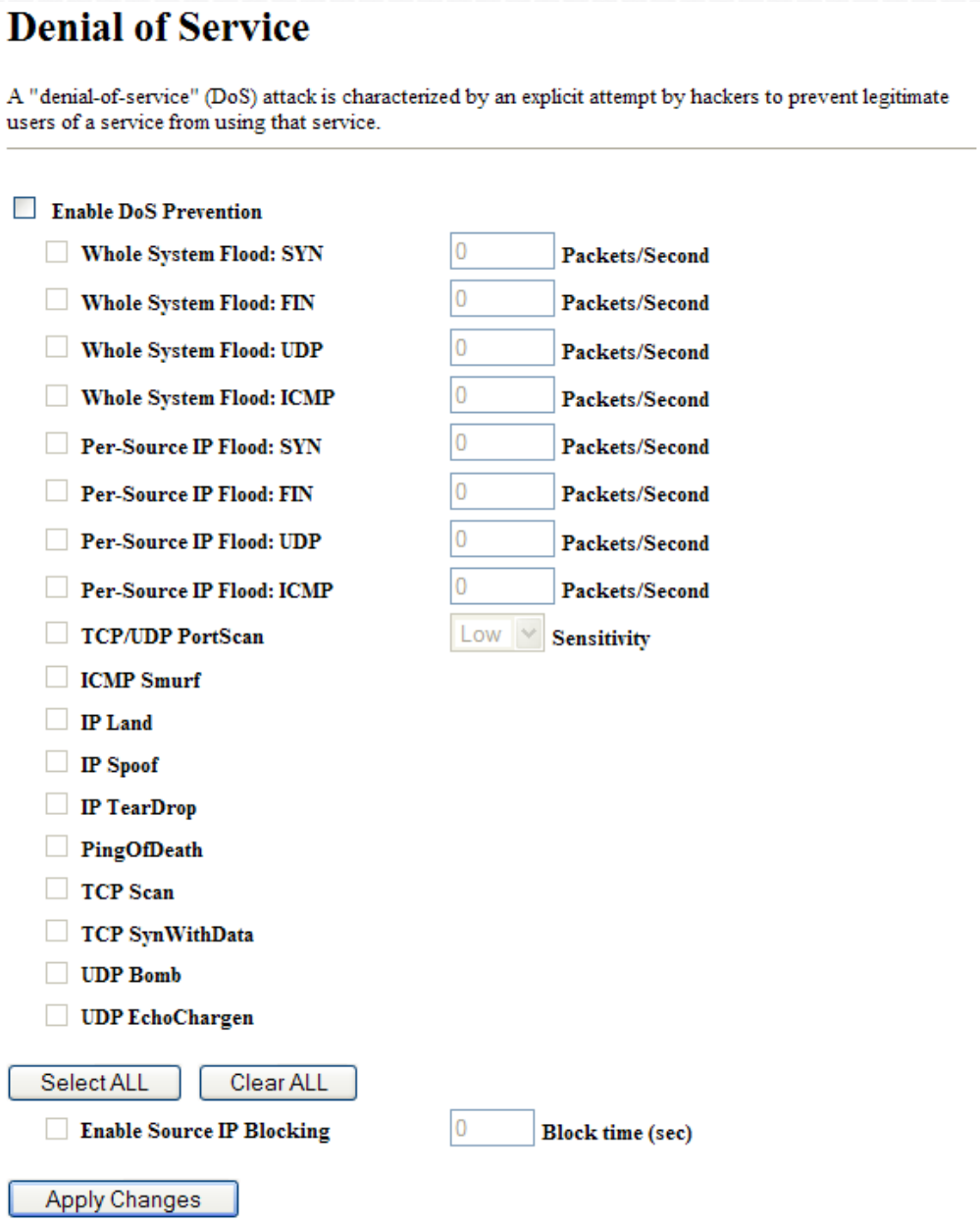

Time Zone Setting
You can maintain the system time by synchronizing with a public time server over the Internet.
Current Time :
Yr 2010 Mon 6 Day 2 Hr 13 Mn 43 Sec 22
Copy Computer Time
Time Zone Select :
(GMT+01:00)Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Enable NTP client update
Automatically Adjust Daylight Saving
NTP server :
192.5.41.41 - North America
(Manual IP Setting)
Apply Change
Reset
Refresh

Item	Description
Current Time	It shows the current time.
Time Zone Select	Click the time zone in your country.
Enable NTP client update	Click the checkbox to enable NTP client update. Refer to 4.26 What is NTP Client?
NTP Server	Click select default or input NTP server IP address.
Apply Change	Click the ***Apply Changes*** button to save and enable NTP client service.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Refresh	Click the refresh the current time shown on the screen.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

3.3.27 Management – Denial-of-Service

This page is used to enable and setup protection to prevent attack by hacker's program. It provides more security for users.



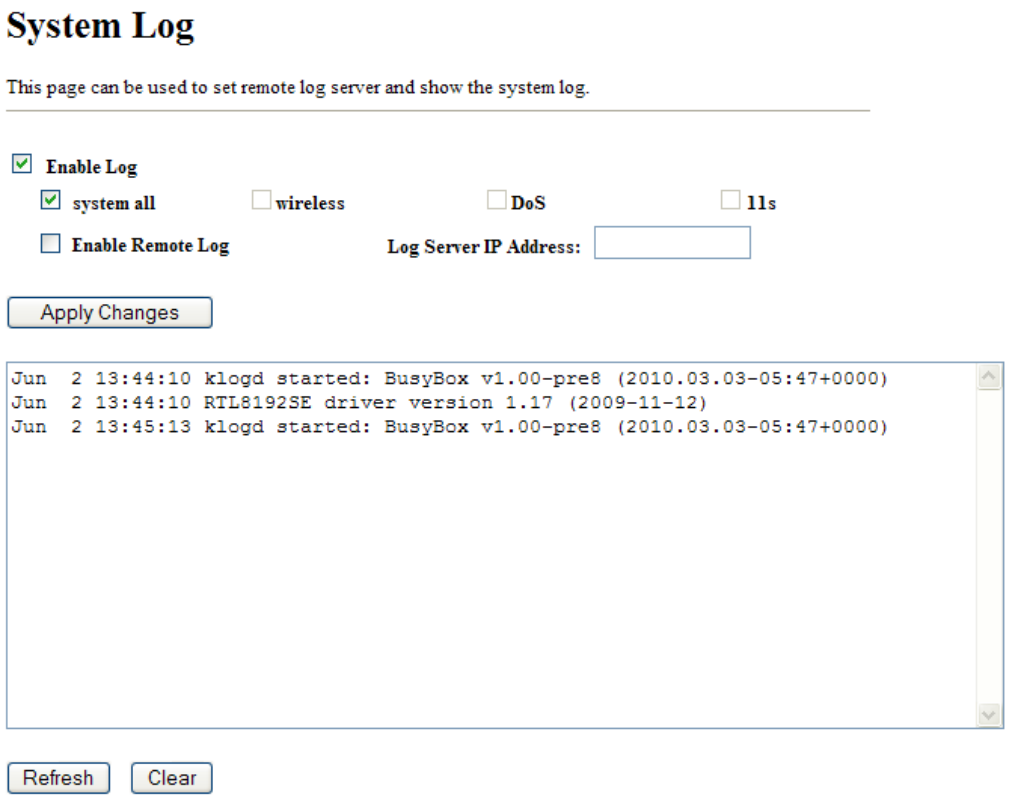
Item	Description
Enable DoS Prevention	Click the checkbox to enable DoS prevention.
Whole System Flood/ Per-Source IP Flood…	Enable and setup prevention in details.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

Select ALL	Click the checkbox to enable all prevention items.
Clear ALL	Click the checkbox to disable all prevention items.
Apply Changes	Click the ***Apply Changes*** button to save above settings.

3.3.28 Management - Log

This page is used to configure the remote log server and shown the current log.



Item	Description
Enable Log	Click the checkbox to enable log.
System all	Show all log of wireless broadband router
Wirelessy	Only show wireless log
DoS	Only show Denial-of-Service log
Enable Remote Log	Click the checkbox to enable remote log service.
Log Server IP Address	Input the remote log IP address

RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

Apply Changes	Click the ***Apply Changes*** button to save above settings.
Refresh	Click the refresh the log shown on the screen.
Clear	Clear log display screen

3.3.29 Management - Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

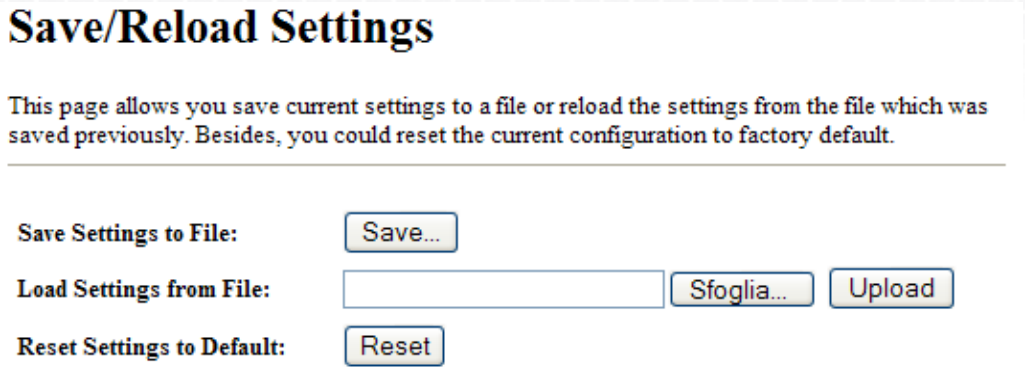
Upgrade Firmware
This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.
Select File:
Sfoglia...
Upload
Reset

Item	Description
Select File	Click the ***Browse*** button to select the new version of web firmware image file.
Upload	Click the ***Upload*** button to update the selected web firmware image to the WLAN Broadband Router.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

3.3.30 Management - Save/ Reload Settings

This page allows you save current settings to a file or reload the settings from the file that was saved previously. Besides, you could reset the current configuration to factory default.

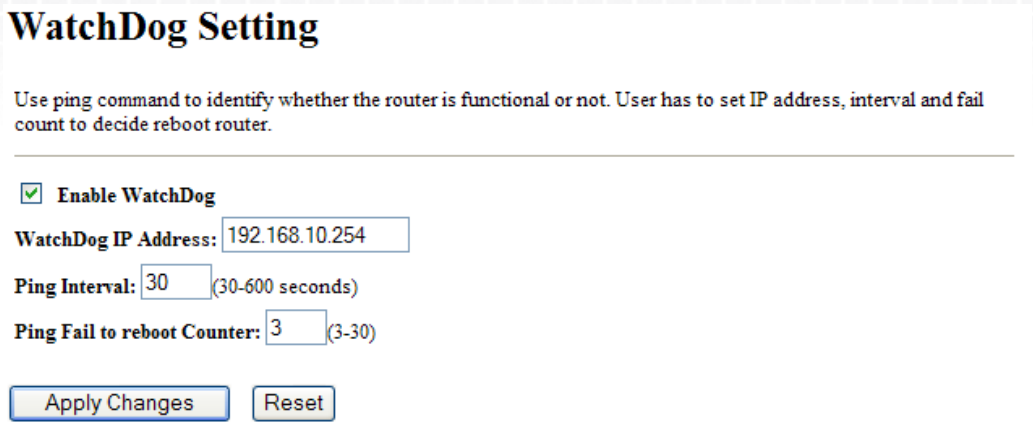

Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
Sfoglia...
Upload
Reset Settings to Default:
Reset

Item	Description
Save Settings to File	Click the ***Save*** button to download the configuration parameters to your personal computer.
Load Settings from File	Click the ***Browse*** button to select the configuration files then click the ***Upload*** button to update the selected configuration to the WLAN Broadband Router.
Reset Settings to Default	Click the ***Reset*** button to reset the configuration parameter to factory defaults.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

3.3.31 Management – Watchdog

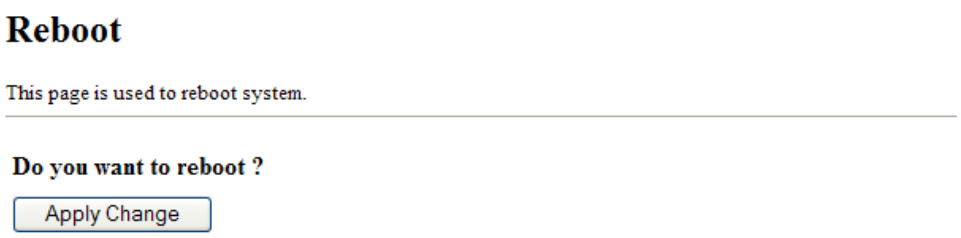
This page is used to do watchdog function using ping command. User set IP address, interval and ping fail count conditions to decide whether router reboots or not.


WatchDog Setting
Use ping command to identify whether the router is functional or not. User has to set IP address, interval and fail count to decide reboot router.
Enable WatchDog
WatchDog IP Address: 192.168.10.254
Ping Interval: 30 (30-600 seconds)
Ping Fail to reboot Counter: 3 (3-30)
Apply Changes
Reset

Item	Description
Enable WatchDog	Click to enable watchdog.
WatchDog IP Address	IP address that is referred.
Ping Interval	Fill in the value by seconds.
Ping Fail to reboot Count	Fill in the value that is the threshold to reboot router when ping fails.
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

3.3.32 Management - Reboot

This page is used to reboot the device.



 Copyright © RayTalk Industries. Tutti i diritti riservati.

3.3.33 Management – Password Setup

This page is used to set the account to access the web server of device. Empty user name and password will disable the protection.

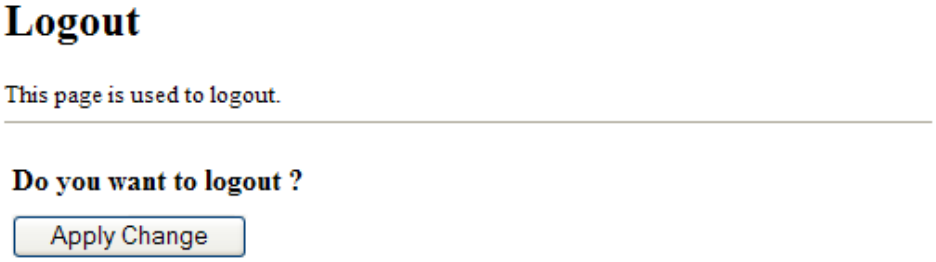
Password Setup
This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.
User Name:
New Password:
Confirmed Password:
Apply Changes
Reset

Item	Description
User Name	Enter the User Name for web management login control.
New Password	Enter the password for web management login control.
Confirmed Password	Enter the password again to confirm the purpose.
Apply Changes	Clear the User Name and Password fields to empty, means to apply no web management login control. Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

3.3.34 Logout

This page is used to logout to device web management.



 Copyright © RayTalk Industries. Tutti i diritti riservati.

Frequently Asked Questions (FAQ)

3.1 What and how to find my PC's IP and MAC address?

IP address is the identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 191.168.1.254 could be an IP address.

The MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN.

To find your PC's IP and MAC address,

- ✓ Open the Command program in the Microsoft Windows.
- ✓ Type in ***ipconfig /all*** then press the ***Enter*** button.

- ➢ Your PC's IP address is the one entitled IP Address and your PC's MAC address is the one entitled Physical Address.

3.2 What is Wireless LAN?

A wireless LAN (WLAN) is a network that allows access to Internet without the need for any wired connections to the user's machine.

3.3 What are ISM bands?

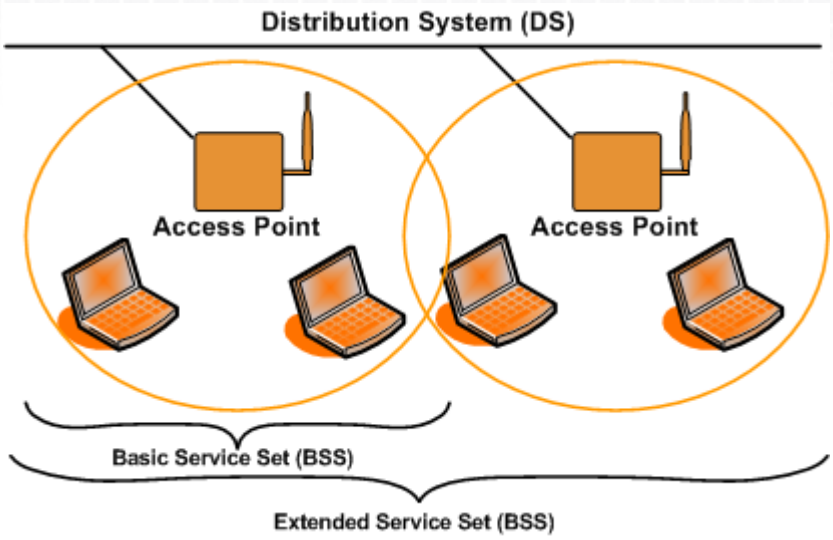
ISM stands for Industrial, Scientific and Medical; radio frequency bands that the Federal Communications Commission (FCC) authorized for wireless LANs. The ISM bands are located at 915 +/- 13 MHz, 2450 +/- 50 MHz and 5800 +/- 75 MHz.

3.4 How does wireless networking work?

The 802.11 standard define two modes: infrastructure mode and ad hoc mode. In infrastructure mode, the wireless network consists of at least one access point connected to the wired network infrastructure and a set of wireless end stations.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

This configuration is called a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or more BSSs forming a single subnetwork. Since most corporate WLANs require access to the wired LAN for services (file servers, printers, Internet links) they will operate in infrastructure mode.



Example 1: wireless Infrastructure Mode

Ad hoc mode (also called peer-to-peer mode or an Independent Basic Service Set, or IBSS) is simply a set of 802.11 wireless stations that communicate directly with one another without using an access point or any connection to a wired network. This mode is useful for quickly and easily setting up a wireless network anywhere that a wireless infrastructure does not exist or is not required for services, such as a hotel room, convention center, or airport, or where access to the wired network is barred (such as for consultants at a client site).

Example 2: wireless Ad Hoc Mode

3.5 What is BSSID?

A six-byte address that distinguishes a particular a particular access point from others. Also know as just SSID. Serves as a network ID or name.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

3.6 What is ESSID?

The Extended Service Set ID (ESSID) is the name of the network you want to access. It is used to identify different wireless networks.

3.7 What are potential factors that may causes interference?

Factors of interference:

- ➢ Obstacles: walls, ceilings, furniture… etc.
- ➢ Building Materials: metal door, aluminum studs.
- ➢ Electrical devices: microwaves, monitors and electrical motors.

Solutions to overcome the interferences:

- ✓ Minimizing the number of walls and ceilings.
- ✓ Position the WLAN antenna for best reception.
- ✓ Keep WLAN devices away from other electrical devices, eg: microwaves, monitors, electric motors, … etc.
- ✓ Add additional WLAN Access Points if necessary.

3.8 What are the Open System and Shared Key authentications?

IEEE 802.11 supports two subtypes of network authentication services: open system and shared key. Under open system authentication, any wireless station can request authentication. The station that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then returns a frame that indicates whether it recognizes the sending station. Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

3.9 What is WEP?

An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. The Wired Equivalent Privacy generates secret shared encryption keys that both source and destination stations can use to alert frame bits to avoid disclosure to eavesdroppers.

WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit.

RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

3.10 What is Fragment Threshold?

The proposed protocol uses the frame fragmentation mechanism defined in IEEE 802.11 to achieve parallel transmissions. A large data frame is fragmented into several fragments each of size equal to fragment threshold. By tuning the fragment threshold value, we can get varying fragment sizes. The determination of an efficient fragment threshold is an important issue in this scheme. If the fragment threshold is small, the overlap part of the master and parallel transmissions is large. This means the spatial reuse ratio of parallel transmissions is high. In contrast, with a large fragment threshold, the overlap is small and the spatial reuse ratio is low. However high fragment threshold leads to low fragment overhead. Hence there is a trade-off between spatial re-use and fragment overhead.

Fragment threshold is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented.

If you find that your corrupted packets or asymmetric packet reception (all send packets, for example). You may want to try lowering your fragmentation threshold. This will cause packets to be broken into smaller fragments. These small fragments, if corrupted, can be resent faster than a larger fragment. Fragmentation increases overhead, so you'll want to keep this value as close to the maximum value as possible.

3.11 What is RTS (Request To Send) Threshold?

The RTS threshold is the packet size at which packet transmission is governed by the RTS/CTS transaction. The IEEE 802.11-1997 standard allows for short packets to be transmitted without RTS/CTS transactions. Each station can have a different RTS threshold. RTS/CTS is used when the data packet size exceeds the defined RTS threshold. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data.

This setting is useful for networks with many clients. With many clients, and a high network load, there will be many more collisions. By lowering the RTS threshold, there may be fewer collisions, and performance should improve.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

Basically, with a faster RTS threshold, the system can recover from problems faster. RTS packets consume valuable bandwidth, however, so setting this value too low will limit performance.

3.12 What is Beacon Interval?

In addition to data frames that carry information from higher layers, 802.11 includes management and control frames that support data transfer. The beacon frame, which is a type of management frame, provides the "heartbeat" of a wireless LAN, enabling stations to establish and maintain communications in an orderly fashion.

Beacon Interval represents the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).

3.13 What is Preamble Type?

There are two preamble types defined in IEEE 802.11 specification. A long preamble basically gives the decoder more time to process the preamble. All 802.11 devices support a long preamble. The short preamble is designed to improve efficiency (for example, for VoIP systems). The difference between the two is in the Synchronization field. The long preamble is 128 bits, and the short is 56 bits.

3.14 What is SSID Broadcast?

Broadcast of SSID is done in access points by the beacon. This announces your access point (including various bits of information about it) to the wireless world around it. By disabling that feature, the SSID configured in the client must match the SSID of the access point.

Some wireless devices don't work properly if SSID isn't broadcast (for example the D-link DWL-120 USB 802.11b adapter). Generally if your client hardware supports operation with SSID disabled, it's not a bad idea to run that way to enhance network security. However it's no replacement for WEP, MAC filtering or other protections.

3.15 What is Wi-Fi Protected Access (WPA)?

Wi-Fi’s original security mechanism, Wired Equivalent Privacy (WEP), has been

 Copyright © RayTalk Industries. Tutti i diritti riservati.

viewed as insufficient for securing confidential business communications. A longer-term solution, the IEEE 802.11i standard, is under development. However, since the IEEE 802.11i standard is not expected to be published until the end of 2003, several members of the WI-Fi Alliance teamed up with members of the IEEE 802.11i task group to develop a significant near-term enhancement to Wi-Fi security. Together, this team developed Wi-Fi Protected Access.

To upgrade a WLAN network to support WPA, Access Points will require a WPA software upgrade. Clients will require a software upgrade for the network interface card, and possibly a software update for the operating system. For enterprise networks, an authentication server, typically one that supports RADIUS and the selected EAP authentication protocol, will be added to the network.

3.16 What is WPA2?

It is the second generation of WPA. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard.

3.17 What is 802.1x Authentication?

802.1x is a framework for authenticated MAC-level access control, defines Extensible Authentication Protocol (EAP) over LANs (WAPOL). The standard encapsulates and leverages much of EAP, which was defined for dial-up authentication with Point-to-Point Protocol in RFC 2284.

Beyond encapsulating EAP packets, the 802.1x standard also defines EAPOL messages that convey the shared key information critical for wireless security.

3.18 What is Temporal Key Integrity Protocol (TKIP)?

The Temporal Key Integrity Protocol, pronounced tee-kip, is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.

3.19 What is Advanced Encryption Standard (AES)?

Security issues are a major concern for wireless LANs, AES is the U.S. government's next-generation cryptography algorithm, which will replace DES and 3DES.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

3.20 What is Inter-Access Point Protocol (IAPP)?

The IEEE 802.11f Inter-Access Point Protocol (IAPP) supports Access Point Vendor interoperability, enabling roaming of 802.11 Stations within IP subnet.

IAPP defines messages and data to be exchanged between Access Points and between the IAPP and high layer management entities to support roaming. The IAPP protocol uses TCP for inter-Access Point communication and UDP for RADIUS request/response exchanges. It also uses Layer 2 frames to update the forwarding tables of Layer 2 devices.

3.21 What is Wireless Distribution System (WDS)?

The Wireless Distribution System feature allows WLAN AP to talk directly to other APs via wireless channel, like the wireless bridge or repeater service.

3.22 What is Universal Plug and Play (uPNP)?

UPnP is an open networking architecture that consists of services, devices, and control points. The ultimate goal is to allow data communication among all UPnP devices regardless of media, operating system, programming language, and wired/wireless connection.

3.23 What is Maximum Transmission Unit (MTU) Size?

Maximum Transmission Unit (MTU) indicates the network stack of any packet is larger than this value will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will be accepted. The actual MTU of the PPP connection will be set to the smaller one of MTU and the peer's MRU. The default is value 1400.

3.24 What is Clone MAC Address?

Clone MAC address is designed for your special application that request the clients to register to a server machine with one identified MAC address.

Since that all the clients will communicate outside world through the WLAN Broadband Router, so have the cloned MAC address set on the WLAN Broadband Router will solve the issue.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

3.25 What is DDNS?

DDNS is the abbreviation of Dynamic Domain Name Server. It is designed for user own the DNS server with dynamic WAN IP address.

3.26 What is NTP Client?

NTP client is designed for fetching the current timestamp from internet via Network Time protocol. User can specify time zone, NTP server IP address.

3.27 What is VPN?

VPN is the abbreviation of Virtual Private Network. It is designed for creating point-to point private link via shared or public network.

3.28 What is IPSEC?

IPSEC is the abbreviation of IP Security. It is used to transferring data securely under VPN.

3.29 What is WLAN Block Relay Between Clients?

An Infrastructure Basic Service Set is a BSS with a component called an *Access Point* (AP). The access point provides a local relay function for the BSS. All stations in the BSS communicate with the access point and no longer communicate directly. All frames are relayed between stations by the access point. This local relay function effectively doubles the range of the IBSS.

3.30 What is WMM?

WMM is based on a subset of the IEEE 802.11e WLAN QoS draft standard. WMM adds prioritized capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different latency and throughput requirements, compete for network resources. By using WMM, end-user satisfaction is maintained in a wider variety of environments and traffic conditions. WMM makes it possible for home network users and enterprise network managers to decide which data streams are most important and assign them a higher traffic priority.

3.31 What is WLAN ACK TIMOUT?

ACK frame has to receive ACK timeout frame. If remote does not receive in specified period, it will be retransmitted.

RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

3.32 What is Modulation Coding Scheme (MCS)?

MCS is Wireless link data rate for 802.11n. The throughput/range performance of a AP will depend on its implementation of coding schemes. MCS includes variables such as the number of spatial streams, modulation, and the data rate on each stream. Radios establishing and maintaining a link must automatically negotiate the optimum MCS based on channel conditions and then continuously adjust the selection of MCS as conditions change due to interference, motion, fading, and other events.

3.33 What is Frame Aggregation?

Every 802.11 packet, no matter how small, has a fixed amount of overhead associated with it. Frame Aggregation combines multiple smaller packets together to form one larger packet. The larger packet can be sent without the overhead of the individual packets. This technique helps improve the efficiency of the 802.11n radio allowing more end user data to be sent in a given time.

3.34 What is Guard Intervals (GI)?

A GI is a period of time between symbol transmission that allows reflections (from multipath) from the previous data transmission to settle before transmitting a new symbol.

The 802.11n draft specifies two guard intervals: 400ns (short) and 800ns (long). Support of the 400ns GI is optional for transmit and receive. The purpose of a guard interval is to introduce immunity to propagation delays, echoes and reflections to which digital data is normally very sensitive.

3.35 What is Mesh protocol?

A wireless mesh network (WMN) is a communications network made up of radio nodes organized in a mesh topology. A wireless mesh network can be seen as a special type of wireless ad-hoc network. A wireless mesh network often has a more planned configuration, and may be deployed to provide dynamic and cost effective connectivity over a certain geographic area. An ad-hoc network, on the other hand, is formed ad hoc when wireless devices come within communication range of each other. It is often assumed that all nodes in a wireless mesh network are immobile, but this may not be the case.

 Copyright © RayTalk Industries. Tutti i diritti riservati.

3.36 Which 3.5G Devices are compatible with RA-M100Plus?

The following 3.5G dongles are fully compatible with RA-M100Plus WAN access:

Huawei

Huawei E220, Huawei E169, Huawei E180, Huawei E172, Huawei E160, Huawei E270, Huawei E230, Huawei E1552, Huawei E156, Huawei E226, Huawei EC168C, Huawei E1750, Huawei E1762, Huawei E1752, Huawei E182E, Huawei K3715, Huawei E170, Huawei E1550

Sierra

Sierra MC8700, Sierra MC8775, Sierra MC8792V, Sierra MC8790, Sierra MC8795V

Option

Option Icon 225, Option Icon 401, Option Icon 505

A-Link

A-Link 3GU, A-Link TITAN

Solomon

Solomon S3GM-690, Solomon S3GM-646, Solomon S3GM-645-11

Sony

Sony Ericsson MD300, Sony Ericsson MD400

ZTE

ZTE MF622, ZTE MF626, ZTE MF636, ZTE MF668

Novatel

Novatel MC950D, Novatel XU870

Other

AnyData ADU 500A, Aiko 82D, Datang D201, Giant D301, Nokia CS-15, SIPTune LM-75, Webee, BandLuxe C120

 Copyright © RayTalk Industries. Tutti i diritti riservati.

4 Configuration Examples

4.1 Example One – PPPoE on the WAN

Sales division of Company ABC likes to establish a WLAN network to support mobile communication on sales' Notebook PCs. MIS engineer collects information and plans the WLAN Broadband Router implementation by the following configuration.

WAN configuration: PPPoE

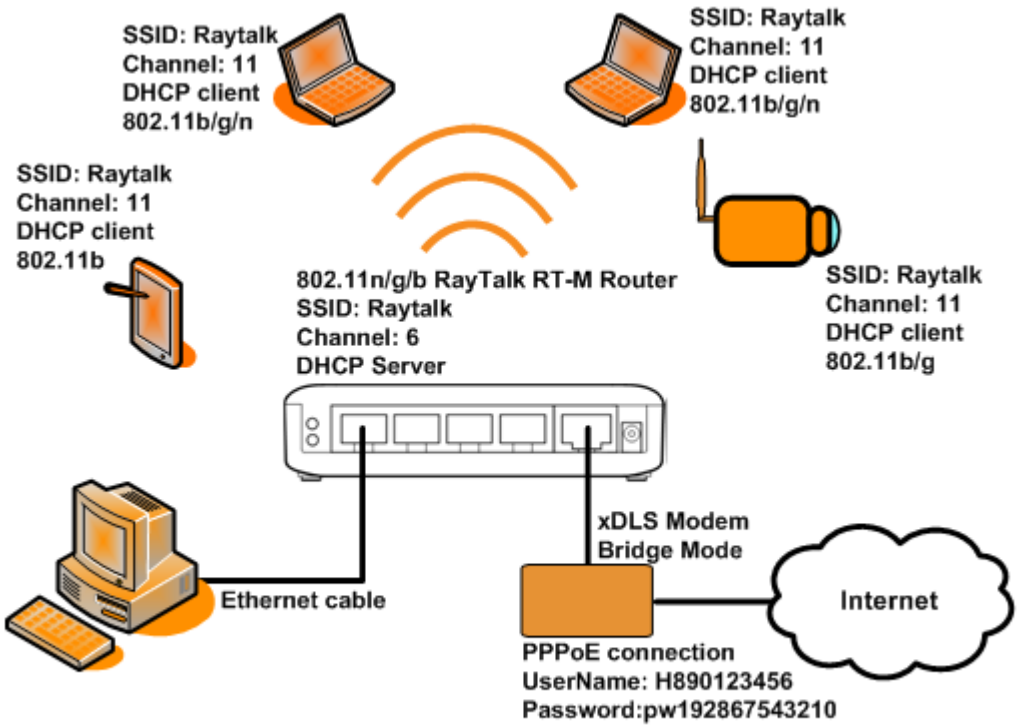
User Name	**H890123456**
Password	**PW192867543210**

LAN configuration

IP Address	**192.168.10.1**
Subnet Mask	**255.255.255.0**
DHCP Client Range	**192.168.10.100 – 192.168.10.200**

WLAN configuration

SSID	**Raytalk**
Channel Number	**6**

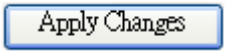


Configuration Example One – PPPoE on the WAN

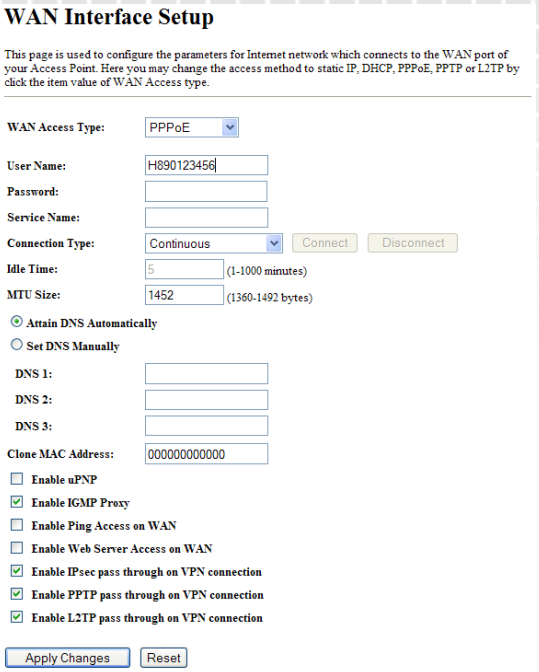
 Copyright © RayTalk Industries. Tutti i diritti riservati.

Configure the WAN interface:

Open WAN Interface Setup page, select PPPoE then enter User Name “**H890123456”** Password “**PW192867543210**”, the password is encrypted to display on the screen.

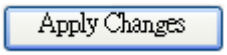


Press button to confirm the configuration setting.

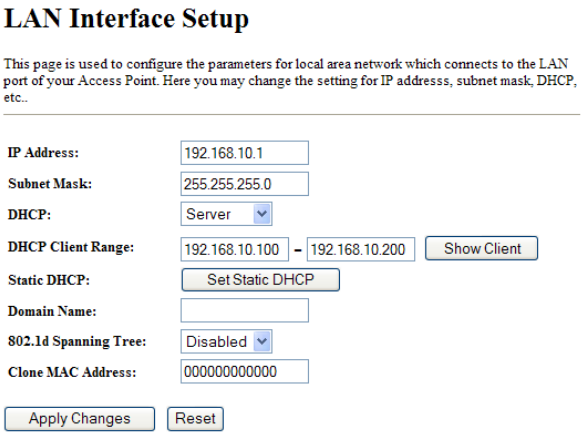

WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.
WAN Access Type: PPPoE
User Name: H890123456
Password:
Service Name:
Connection Type: Continuous Connect Disconnect
Idle Time: 5 (1-1000 minutes)
MTU Size: 1452 (1360-1492 bytes)
Attain DNS Automatically
Set DNS Manually
DNS 1:
DNS 2:
DNS 3:
Clone MAC Address: 000000000000
Enable uPNP
Enable IGMP Proxy
Enable Ping Access on WAN
Enable Web Server Access on WAN
Enable IPsec pass through on VPN connection
Enable PPTP pass through on VPN connection
Enable L2TP pass through on VPN connection
Apply Changes Reset

Configure the LAN interface:

Open LAN Interface Setup page, enter the IP Address “**192.168.10.1**”, Subnet Mask “**255.255.255.0**”, DHCP Server, DHCP client range “**192.168.10.100**” to “**192.168.10.200**”.



Press button to confirm the configuration setting.

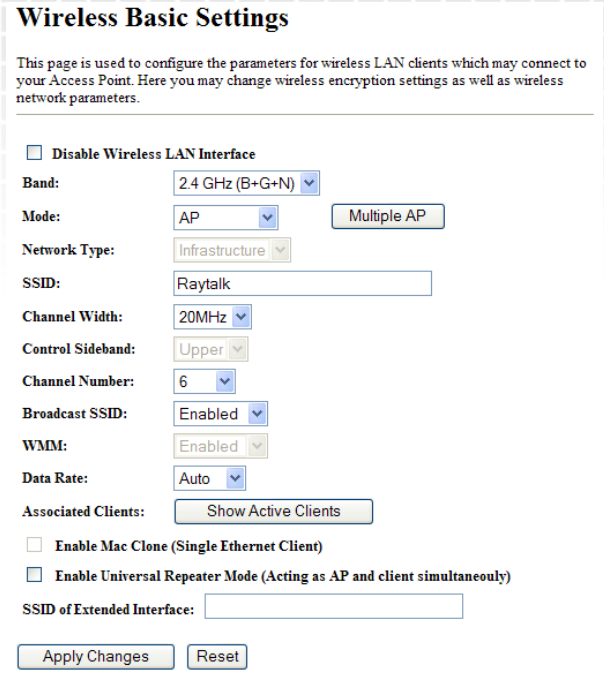

LAN Interface Setup
This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..
IP Address: 192.168.10.1
Subnet Mask: 255.255.255.0
DHCP: Server
DHCP Client Range: 192.168.10.100 - 192.168.10.200 Show Client
Static DHCP: Set Static DHCP
Domain Name:
802.1d Spanning Tree: Disabled
Clone MAC Address: 000000000000
Apply Changes Reset

RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

Configure the WLAN interface:

Open WLAN Interface Setup page, enter the SSID "**Raytalk**", Channel Number "**6**".

Press button to confirm the configuration setting.



 Copyright © RayTalk Industries. Tutti i diritti riservati.

4.2 Example Two – Fixed IP on the WAN

Company ABC likes to establish a WLAN network to support mobile communication on all employees' Notebook PCs. MIS engineer collects information and plans the WLAN Broadband Router implementation by the following configuration.

WAN configuration: Fixed IP

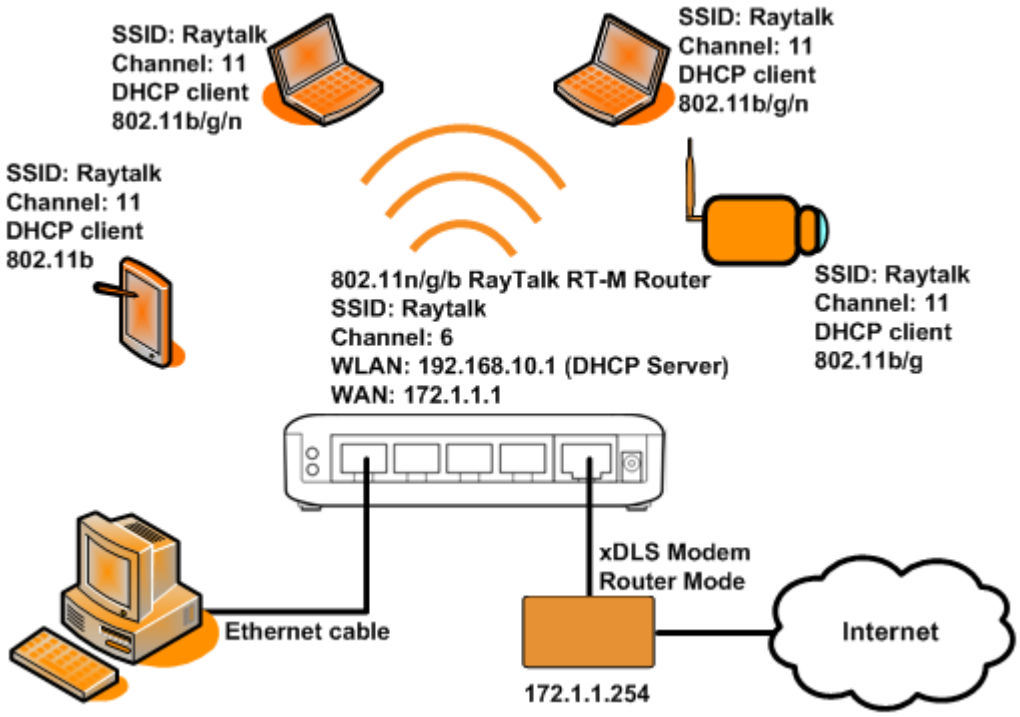
IP Address	**172.1.1.1**
Subnet Mask	**255.255.255.0**
Default Gateway	**172.1.1.254**

LAN configuration

IP Address	**192.168.1.1**
Subnet Mask	**255.255.255.0**
DHCP Client Range	**192.168.10.100 – 192.1680.1.200**

WLAN configuration

SSID	**Raytalk**
Channel Number	**6**



Configuration Example Two – Fixed IP on the WAN

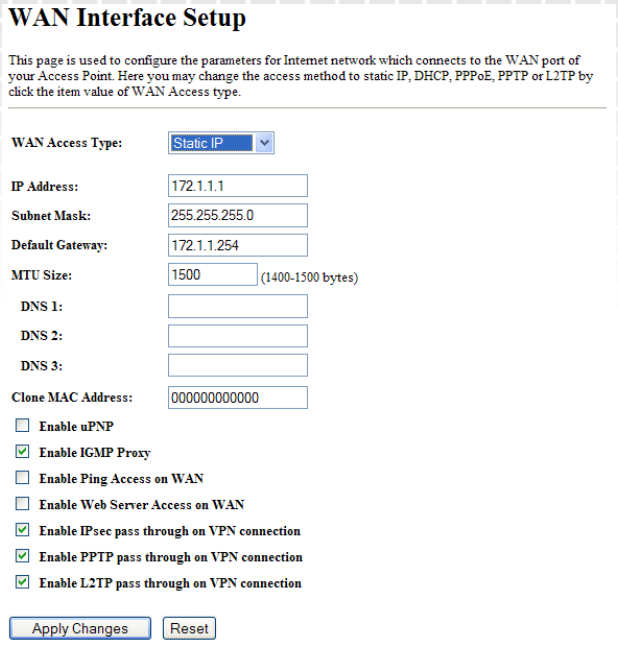
RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

Configure the WAN interface:

Open WAN Interface Setup page, select Fixed IP then enter IP Address "**172.1.1.1",** subnet mask "**255.255.255.0**", Default gateway "**172.1.1.254**".

Apply Changes

Press button to confirm the configuration the setting.

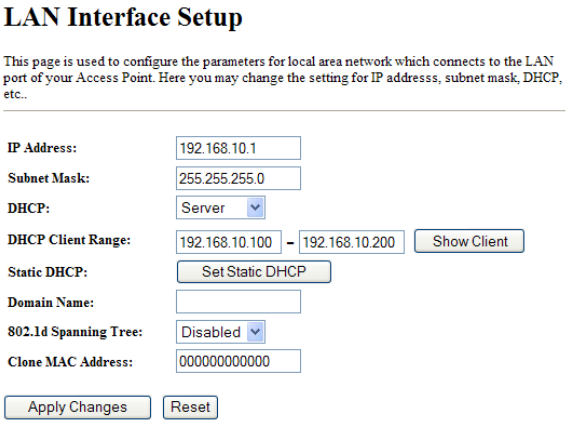

WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.
WAN Access Type:
Static IP
IP Address:
172.1.1.1
Subnet Mask:
255.255.255.0
Default Gateway:
172.1.1.254
MTU Size:
1500
(1400-1500 bytes)
DNS 1:
DNS 2:
DNS 3:
Clone MAC Address:
000000000000
Enable uPNP
Enable IGMP Proxy
Enable Ping Access on WAN
Enable Web Server Access on WAN
Enable IPsec pass through on VPN connection
Enable PPTP pass through on VPN connection
Enable L2TP pass through on VPN connection
Apply Changes
Reset

Configure the LAN interface:

Open LAN Interface Setup page, enter the IP Address "**192.168.10.1**", Subnet Mask "**255.255.255.0**", enable DHCP Server, DHCP client range "**192.168.10.100**" to "**192.168.10.200**".

Apply Changes

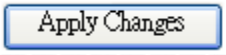
Press button to confirm the configuration setting.



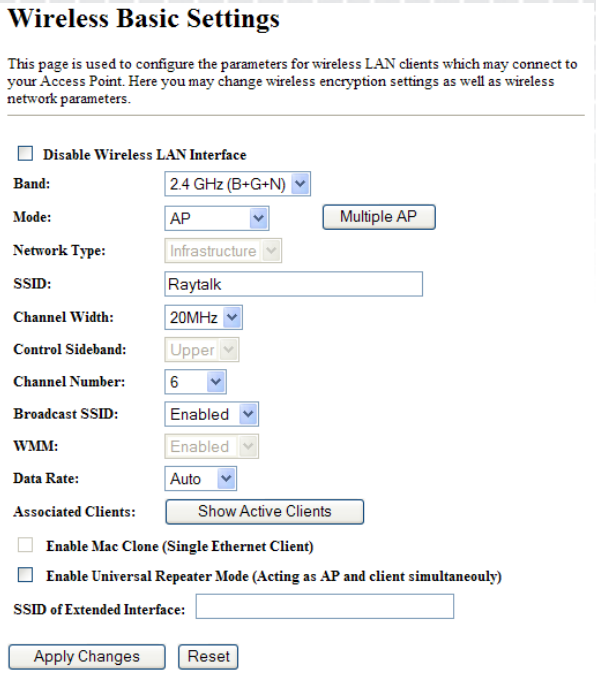
RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

Configure the WLAN interface:

Open WLAN Interface Setup page, enter the SSID "**Raytalk**", Channel Number "6".



Press button to confirm the configuration setting.



 Copyright © RayTalk Industries. Tutti i diritti riservati.

4.3 Example Three (RA-M100Plus only) – 3.5G on the WAN

Company ABC likes to establish a WLAN network to support mobile communication on all employees' Notebook PCs. MIS engineer collects information and plans the WNAP 3G Mobile Router implementation by the following configuration.

WAN configuration: Fixed IP

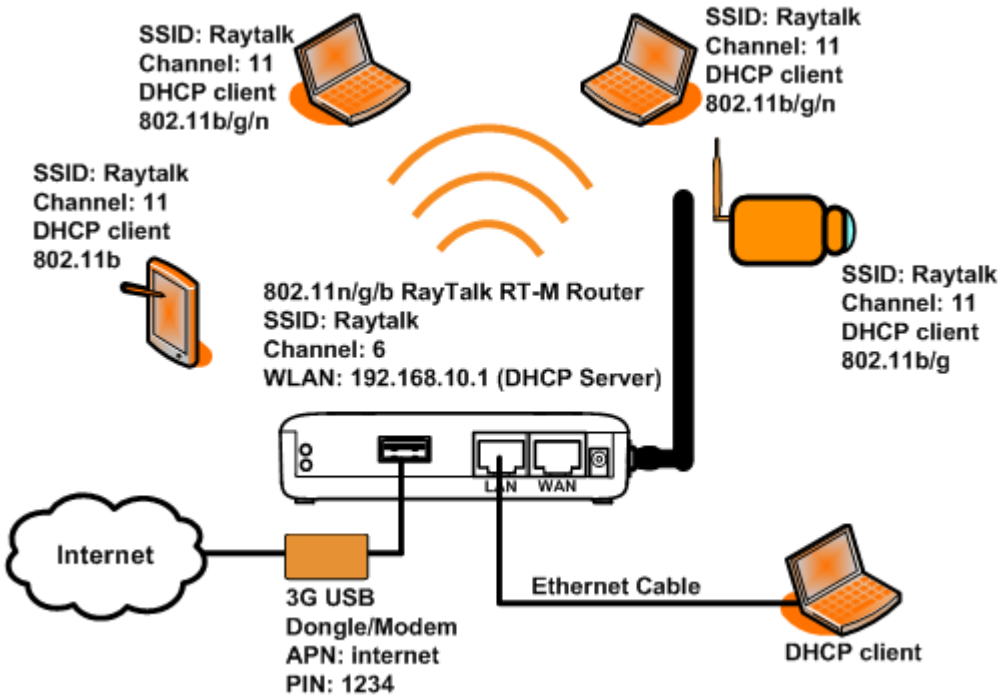
3.5G Device	**Huawei E220** (for example)
Authorization Number	***99#**
APN	**internet**
PIN	**1234**

LAN configuration

IP Address	**192.168.10.1**
Subnet Mask	**255.255.255.0**
DHCP Gateway	**192.168.10.1**
DHCP Client Range	**192.168.10.100 – 192.168.10.200**

WLAN configuration

SSID	**Raytalk**
Channel Number	**6**



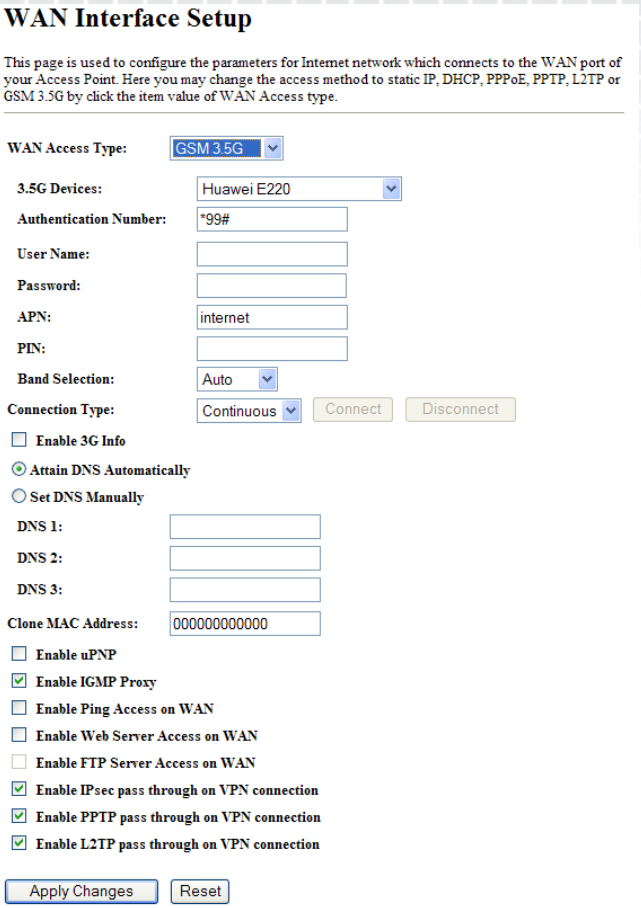
Configuration Example Three – 3.5G on the WAN

RayTalk Industries www.raytalk.com Copyright © RayTalk Industries. Tutti i diritti riservati.

Configure the WAN interface:

Open WAN Interface Setup page, select GSM 3.5 then select 3.5G Device “Huawei E220”. Enter Authentication Number “***99#**”, APN “**internet**” and PIN “**1234**”.

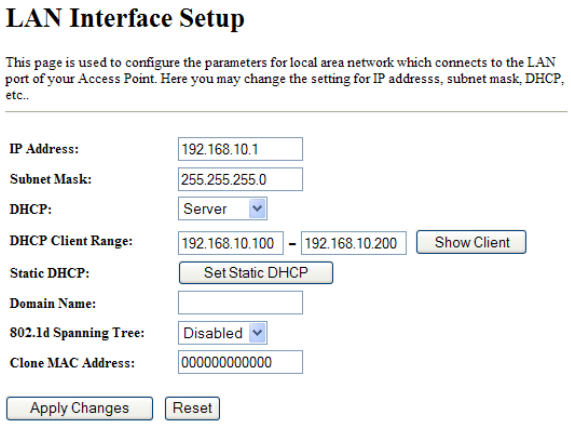
Press button to confirm the configuration the setting.


WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP, L2TP or GSM 3.5G by click the item value of WAN Access type.
WAN Access Type: GSM 3.5G
3.5G Devices: Huawei E220
Authentication Number: *99#
User Name:
Password:
APN: internet
PIN:
Band Selection: Auto
Connection Type: Continuous Connect Disconnect
Enable 3G Info
Attain DNS Automatically
Set DNS Manually
DNS 1:
DNS 2:
DNS 3:
Clone MAC Address: 000000000000
Enable uPNP
Enable IGMP Proxy
Enable Ping Access on WAN
Enable Web Server Access on WAN
Enable FTP Server Access on WAN
Enable IPsec pass through on VPN connection
Enable PPTP pass through on VPN connection
Enable L2TP pass through on VPN connection
Apply Changes
Reset

Configure the LAN interface:

Open LAN Interface Setup page, enter the IP Address “**192.168.10.1**”, Subnet Mask “**255.255.255.0**”, enable DHCP Server, DHCP client range “**192.168.10.100**” to “**192.168.10.200**”.

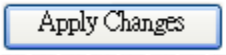
Press button to confirm the configuration setting.


LAN Interface Setup
This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..
IP Address: 192.168.10.1
Subnet Mask: 255.255.255.0
DHCP: Server
DHCP Client Range: 192.168.10.100 – 192.168.10.200 Show Client
Static DHCP: Set Static DHCP
Domain Name:
802.1d Spanning Tree: Disabled
Clone MAC Address: 000000000000
Apply Changes
Reset

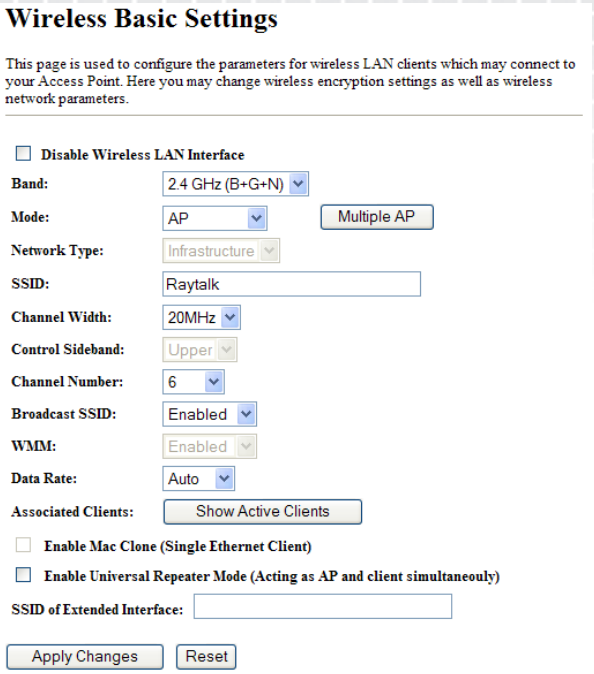
 Copyright © RayTalk Industries. Tutti i diritti riservati.

Configure the WLAN interface:

Open WLAN Interface Setup page, enter the SSID "**Raytalk**", Channel Number "6".



Press button to confirm the configuration setting.



 Copyright © RayTalk Industries. Tutti i diritti riservati.